EXHIBIT 2

UNITED STATES OF AMERICA
FINANCIAL CRIMES ENFORCEMENT NETWORK
DEPARTMENT OF THE TREASURY

IN THE MATTER OF:	)	
	)	**Number 2023-04**
Binance Holdings Limited,	)	
Binance (Services) Holdings Limited,	)	
Binance Holdings (IE) Limited,	)	
d/b/a Binance and Binance.com	)	

CONSENT ORDER IMPOSING CIVIL MONEY PENALTY

The Financial Crimes Enforcement Network (FinCEN) has conducted a civil enforcement investigation and determined that grounds exist to impose a Civil Money Penalty on Binance Holdings Limited, Binance (Services) Holdings Limited, and Binance Holdings (IE) Limited, collectively doing business as Binance and Binance.com[1] for violations of the Bank Secrecy Act (BSA) and its implementing regulations.[2] Binance admits only to the facts admitted in the November 21, 2023 Plea Agreement of Binance Holdings Limited with the United States Department of Justice (DOJ) for conduct from August 2017 through October 2022 and neither admits nor denies the remainder of the facts set forth herein. Binance consents to the issuance of

[1] Each of the legal entities in the above list is: (i) affiliated through common ownership and control by the same individual, and (ii) is involved—such as through ownership of intellectual property, provision of technology services, or employment of personnel—in the coordinated operation of the Binance.com convertible virtual currency (CVC) exchange, which serves as the public face of these companies and the vehicle through which they provide financial services to customers. In addition to these companies, other legal entities (including those described in this Consent Order) have also been involved in the operation of the Binance.com CVC exchange; for purposes of resolving its investigation, FinCEN agreed to enter into a Consent Order with the three legal entities listed above. The CEO of the Binance.com business is the same individual who beneficially owns these legal entities. The conduct described herein relates to the operation of the Binance.com CVC exchange, and the term Binance is generally used to refer to this business. In certain instances, this Order uses Binance's "doing business as" name of Binance.com, primarily to differentiate the Binance.com CVC exchange from the Binance.us CVC exchange.

[2] The BSA is codified at 12 U.S.C. §§ 1829b, 1951-1960, 31 U.S.C. §§ 5311-5314, 5316-5336 and includes other authorities reflected in notes thereto. Regulations implementing the BSA appear at 31 C.F.R. Chapter X.

this Consent Order, agrees to pay the civil money penalty imposed in this Consent Order, and agrees to comply with the Undertakings and Monitor requirements and the other provisions of this Consent Order.

I. JURISDICTION

Overall authority for enforcement and compliance with the BSA lies with the Director of FinCEN, and the Director may impose civil penalties for violations of the BSA and its implementing regulations.[3]

At all times relevant to this Consent Order, Binance was a "domestic financial institution," specifically a "money services business" (MSB) as defined by the BSA and its implementing regulations.[4] As such, Binance was required to comply with applicable BSA regulations.

II. STATEMENT OF FACTS

The conduct described below took place from on or about July 14, 2017[5] through July 30, 2023 (the Relevant Time Period), unless otherwise indicated.[6]

[3] 31 U.S.C. § 5321(a); 31 C.F.R. §§ 1010.810(a), (d); Treasury Order 180-01 (July 1, 2014, reaff'd January 14, 2020).

[4] 31 C.F.R. § 1010.100(ff) (defining "money services business").

[5] As explained below, from its launch on July 14, 2017, Binance was required to identify and report to FinCEN suspicious transactions relevant to a possible violation of law or regulation. *See* 31 C.F.R. § 1022.320. Additionally, within 90 days of Binance's business being established (no later than October 12, 2017), Binance was required to develop, implement, and maintain an effective Anti-Money Laundering program that is reasonably designed to prevent Binance from being used to facilitate money laundering and the financing of terrorist activities. *See* 31 C.F.R. § 1022.210. Finally, within 180 days of its business being established (no later than January 10, 2018), Binance was required to register as a money services business with FinCEN. *See* 31 C.F.R. § 1022.380.

[6] The Relevant Time Period for the Department of Justice resolution with Binance is January 1, 2018 through October 31, 2022.

A. Binance and its CVC Platforms

1. *The Binance.com Platform*

Binance's main platform was launched in 2017 and was accessible to customers through the Binance.com website.[7] The platform currently has five primary CVC trading pairs—bitcoin, ether, litecoin, tether, and Binance Coin (BNB). These CVCs are offered with over 160 separate CVCs in over 580 trading pairs. After launching as a CVC-to-CVC exchange, Binance also began providing fiat-to-CVC trading.

Shortly after its 2017 launch, Binance quickly became one of the largest CVC exchanges by daily trading volume. According to public reporting, Binance processed over $9.5 trillion in trading volume in 2021, or roughly half of all spot trading volume handled by centralized CVC exchanges. Despite a market downturn in 2022, Binance processed spot trades in excess of $5.2 trillion and generally increased its market share during the year to roughly 60% of all centralized CVC exchanges' spot trading volume. Binance maintained a similar share of the market for trading of CVC derivatives on centralized exchanges. Third-party rankings of CVC exchanges by volume continue to consistently identify Binance as processing more volume per day than roughly the next 9 CVC exchanges combined. Binance customers include both individuals (Retail Users) and businesses (Enterprise Users). Binance advertises its ability to process 100 orders per 10 seconds through its Application Programming Interface (API) and 200,000 orders per 24 hours.

[7] Although FinCEN refers to such persons using the term "customer," Binance more commonly refers to its customers as "users." For purposes of this Consent Order, the two terms are used interchangeably.

2. *The Binance.us Platform*[8]

In September 2019, Binance launched a second platform focused on the U.S. and accessible to U.S. customers through the Binance.us website. This U.S.-focused platform was operated by BAM Trading Services, Inc., a Binance-affiliated entity that registered with FinCEN in December 2019. Although both Binance.com and Binance.us are CVC exchanges, Binance.us offers a more limited suite of products (*e.g.*, fewer CVC trading pairs, no derivative products, etc.) and processes a much smaller amount of CVC trading than Binance.com does. Binance.us is an affiliate, but not a subsidiary, of the entities doing business as Binance.

B. FinCEN

FinCEN is a bureau within the U.S. Department of the Treasury and is the federal authority that enforces the BSA by investigating and imposing civil money penalties on financial institutions and individuals for willful violations of the BSA.[9] As delegated by the Secretary of the Treasury, FinCEN has "authority for the imposition of civil penalties" and "[o]verall authority for enforcement and compliance. . . ."[10]

C. Bank Secrecy Act Requirements

The term "money services business" is defined in 31 C.F.R. § 1010.100(ff) as any of the following categories of business: (1) dealers in foreign exchange; (2) check cashers; (3) issuers or

[8] The violations described in this Consent Order relate to the operation of the Binance.com CVC exchange. However, as explained below, Binance's plan in establishing Binance.us and subsequent operation of this CVC exchange is relevant to Binance's failure to register with FinCEN.

[9] 31 U.S.C. § 5321(a). In civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1), to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the BSA, or that the entity or individual otherwise acted with an improper motive or bad purpose. With respect to FinCEN's Consent Order, Binance admits to "willfulness" only as the term is used in civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1).

[10] 31 C.F.R. § 1010.810(a), (d).

sellers of traveler's checks or money orders; (4) providers of prepaid access; (5) money transmitters; (6) U.S. Postal Service; or (7) sellers of prepaid access.[11] The regulations define the term "money transmitter" as a person that either "provides money transmission services" or who is otherwise "engaged in the transfer of funds."[12] "Money transmission services" are defined in FinCEN's regulations as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[13] A foreign-located business is an MSB if it does business "wholly or in substantial part within the United States."[14] Given these definitions and Binance's activities within the United States, Binance was a "domestic financial institution," specifically a "money services business," including a "money transmitter," operating in the United States.[15] As a result, Binance was required to comply with FinCEN's regulations applicable to MSBs during the Relevant Time Period.

Registration: The BSA and its implementing regulations require an MSB, such as Binance, to register as an MSB with FinCEN within 180 days of beginning operations and to renew that registration every two years.[16]

[11] 31 C.F.R. § 1010.100(ff).

[12] 31 C.F.R. § 1010.100(ff)(5).

[13] 31 C.F.R. § 1010.100(ff)(5).

[14] 31 U.S.C. §§ 5312(a)(6), 5312(b), 5330(d); 31 C.F.R. § 1010.100(ff).

[15] *See* 31 U.S.C. § 5312(b)(1) (defining domestic financial institution); 31 C.F.R. §§ 1010.100(ff) (defining "money services business") and 1010.100(ff)(5) (defining "money transmitter"). FinCEN also issued interpretive guidance explaining why CVC exchangers are money transmitters. *See* FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013; FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019.

[16] 31 U.S.C. § 5330 and 31 C.F.R. §§ 1022.380(b)(2) and (3).

AML Program: The BSA and its implementing regulations require an MSB, such as Binance, to develop, implement, and maintain an effective Anti-Money Laundering (AML) program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.[17] Binance was required to develop, implement and maintain an effective, written AML program that, at a minimum: (1) incorporates policies, procedures and internal controls reasonably designed to assure ongoing compliance with the BSA and its implementing regulations; (2) designates an individual responsible to assure day-to-day compliance with the MSB's AML program and all BSA regulations; (3) provides education and/or training for appropriate personnel, including training in the detection of suspicious transactions; and (4) provides for independent review to monitor and maintain an adequate program.[18]

Suspicious Activity Reporting: The BSA and its implementing regulations require an MSB, such as Binance, to identify and report suspicious transactions relevant to a possible violation of law or regulation in SARs filed with FinCEN. Specifically, the BSA and its implementing regulations require MSBs to report transactions that involve or aggregate to at least $2,000, are conducted by, at, or through the MSB, and that the MSB "knows, suspects, or has reason to suspect" are suspicious.[19] A transaction is "suspicious" if an MSB "knows, suspects, or has reason to suspect" the transaction: (a) involves funds derived from illegal activities, or is conducted to disguise funds derived from illegal activities; (b) is designed to evade the reporting or recordkeeping requirements of the BSA or regulations implementing it; or (c) has no business or

[17] 31 U.S.C. § 5318(h); 31 C.F.R. § 1022.210(a).

[18] 31 U.S.C. § 5318(h)(1); 31 C.F.R. § 1022.210(d) and (e) ("A [MSB] must develop and implement an [AML] program that complies with the requirements of this section on or before . . . the end of the 90-day period beginning on the day following the date the business is established.").

[19] 31 U.S.C. § 5318(g); 31 C.F.R. § 1022.320.

apparent lawful purpose or is not the sort in which the customer normally would be expected to engage, and the MSB knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose of the transaction.[20] An MSB is generally required to file a SAR no later than 30 calendar days after the initial detection by the MSB of the facts that may constitute a basis for filing a SAR.[21]

D. Binance Did Business in the U.S. as an Unregistered MSB

At no time did Binance register with FinCEN. Yet throughout the Relevant Time Period, Binance did business as a money transmitter in substantial part within the United States, including by cultivating and serving over 1 million U.S. customers through its main platform, Binance.com, which solicited and accepted orders to convert CVC through CVC-to-CVC trades, as well as CVC-to-fiat currency trades. In connection with these activities, Binance accepted deposits from customers, and, otherwise, accepted money or property, including CVC, to margin, guarantee, or secure trades on Binance.com. As explained in greater detail below, Binance provided these CVC services to U.S. customers, including by allowing persons located in the U.S. to access the Binance.com platform and by exchanging their CVC or fiat currency on the platform.

During the Relevant Time Period and as a result of the flawed controls that Binance deployed (described below), Binance maintained over 1 million U.S. users on the Binance.com platform. Although many of these were Retail Users, a large number were Enterprise Users, which include market makers and liquidity providers, who engage in high levels of activity on the Binance.com platform and were a crucial element in Binance's commercial success. Accordingly, even as the *total number* of U.S. users appears to have fluctuated during the Relevant Time Period,

[20] 31 C.F.R. § 1022.320(a)(2)(i)-(iii).

[21] 31 C.F.R. § 1022.320(b)(3).

the *trading volume* of U.S. users, which was largely driven by Enterprise Users, continued to rise through mid-2021. Binance's own estimates of this peak identified U.S. Enterprise Users trading more than 650,000 bitcoin of CVC in a single month in late 2021, which had a prevailing USD-equivalent value in excess of $35 billion.

As explained in more detail below, Binance's substantial business in the United States throughout the Relevant Time Period was a result of ineffective controls and a willful failure to cease serving U.S. customers (including taking steps to obscure the continuing presence of U.S. users on Binance.com), despite assuring a state regulator that it had done so. As detailed in each of the corresponding subsections below, Binance: (i) maintained U.S.-based personnel and other operational touchpoints to the United States; (ii) operated for over two years with no geofencing controls to restrict access by U.S. users, and then employed flawed protocols to "ringfence" the Binance.com platform from U.S. users while misleading U.S. authorities; (iii) circumvented its own "ringfencing" protocols to allow large U.S. firms to continue to operate on the Binance.com platform, including by directly instructing clients on how to change their KYC[22] and use virtual private networks (VPNs)[23] to obfuscate U.S. ties and indirectly through the maintenance of accounts for a subset of Enterprise Users some of which acted as conduits for U.S. users (Exchange Brokers); and (iv) devising a scheme to retain lucrative U.S. users while redirecting regulatory focus through the establishment of Binance.us (a U.S.-located MSB registered with FinCEN that

[22] KYC, or Know Your Customer, refers to the information that financial institutions collect from their customers to document and understand basic information about the customer and its intended relationship with the financial institution.

[23] A VPN has the effect of "masking" a user's true IP address. Financial institutions often use IP addresses to determine the jurisdiction from which a user has accessed its website or mobile application which can then be used as part of the financial institution's "geofencing controls" to identify and block or restrict access, including to support efforts by the financial institution to "ringfence" itself from certain jurisdictions (*e.g.*, higher risk jurisdictions or those in which it has elected to not obtain a license or register to do business). However, such controls can be rendered ineffective as the result of VPN masking (particularly when, as here, the financial institution instructs customers on how to use VPNs to circumvent geofencing controls).

purports to be Binance's sole presence in the United States and separate from Binance.com, but that in reality lacked autonomy and maintained extensive ties to Binance.com).

1. *Binance Maintained U.S.-based Personnel and Other Operational Touchpoints to the United States*

In addition to the extensive number of, and trading volume associated with, U.S. users that Binance improperly retained without registering with FinCEN, numerous other factors indicate that Binance engaged in money transmitting activities in the United States, including: (i) employing more than 100 individuals who are based in the United States, including senior personnel, such as an advisor to Binance's CEO, several c-suite executives (former Chief Business Officer, former Chief Strategy Officer, Chief Technology Officer), Global Director of Brand Marketing, and Vice President of Global Expansion Operations; (ii) until recently, partnering with a U.S. financial institution to offer its users a USD-based stablecoin, which, as of November 2022 had a circulating supply of more than $23 billion; and (iii) acquiring a U.S. company to provide its users with CVC wallet services. In connection with its resolution with FinCEN, Binance agreed to remediate these connections to the U.S.

2. *Binance's Delayed and Flawed "Ringfencing" of the United States and Misleading Approach to U.S. Regulatory Inquiries*

During much of the Relevant Time Period, Binance's geofencing controls were either nonexistent, or were superficial and ineffective: starting in the summer of 2019 (two years after Binance.com launched), U.S. users were identified based on their IP addresses, but users accessing Binance.com from a U.S. IP address were not fully blocked. Instead, those users needed only to "self-certify" that they were not U.S. persons. Until January 2021, Binance processed transactions with U.S. persons who completed this self-certification, even where Binance possessed information contrary to their certification. Moreover, Binance did not even purport to revoke the ability of many U.S. Enterprise Users to access the Binance.com API until August 2021, and, as

will be explained in the subsections that follow, this revocation did not apply to many of the most commercially lucrative U.S. Enterprise Users in Binance's VIP program. As also described below, Binance's VIP U.S. users also benefited from deliberate actions by Binance personnel to conceal their use of the Binance.com exchange.

Despite Binance's knowledge of those flaws, however, Binance represented to regulators that it was not serving U.S. customers. In May 2018, Binance assured a U.S. authority that it "did not maintain business operations within the [jurisdiction]." Further, in August 2019, Binance was asked to provide a partner company's state regulator with information about Binance's geofencing controls. Its response contained false or misleading statements about these controls. For example, Binance stated in its August 2019 response that it detects user IP addresses and "blocks those it determines are based in the U.S.," but Binance made no such determination apart from simply accepting a "self-certification" that a customer is not a U.S. person. Additionally, Binance stated that if a customer used a VPN to mask their IP address, Binance "employs a secondary manual control during the KYC process to check for U.S. persons." At the time of Binance's response, however, the vast majority of users on the platform were not required to undergo KYC, and Binance had no such secondary manual control applicable to users accessing Binance through a VPN, whether required to undergo KYC or not. In fact, Binance took no meaningful steps to limit its U.S. presence until more than two years after launch, and well over a year after it was contacted by a U.S. authority.

3. *Binance Helped U.S. Users Circumvent Its Own "Ringfencing"*

Binance not only knew of the flaws in its "ringfencing" controls, but it developed a plan to actively assist and encourage its U.S. VIP users to exploit them. From its launch in 2017, Binance catered to higher volume, commercially important users through its "VIP Program," which offered favorable trading fees and higher limits on the number of orders that users could submit through

the Binance.com exchange. Binance thus had significant commercial motivations to go to great lengths to support these VIP users. Binance's internal reports indicated that, in 2019, VIP users consistently accounted for between two-thirds and three-quarters of both trading volume and trading revenue on Binance.com.

In 2019, Binance even developed a process to notify VIP users if they became the subject of a law enforcement inquiry. This process provided for members of Binance's VIP team to "contact the user through all available means (text, phone), to inform him/her that his account has been frozen or unfrozen. . . .***We cannot in any circumstances directly tell the user to run/withdraw, we can get sued or undertake personal liability. Giving a strong hint[,] such as your account is unlocked/your account has been investigated by XXX is usually a good enough hint of severity***."

U.S users represented a crucial element of the VIP userbase, at times accounting for roughly 15 to 20% of Binance's transaction fees. In October 2020, a single U.S. VIP user was responsible for 12% of all trading volume on Binance.com.

In the summer of 2019, as Binance prepared to launch Binance.us and roll out the initial controls applicable to U.S. users accessing Binance.com, Binance senior management conducted a series of meetings to discuss how to facilitate the evasion of its ringfencing by certain U.S. VIP users. As discussed in the meetings, the approach would vary based on whether the U.S. VIP user had already completed KYC with Binance. If a U.S. VIP user had already provided Binance with KYC documents demonstrating its U.S. nexus, Binance would reach out "privately" to obtain new KYC documents showing that the entity was in an offshore jurisdiction. For U.S. VIP users who had not yet completed KYC (and were identified as being U.S. users based on their IP address), Binance personnel would encourage such users to "change their IP." In practice, this meant using

a VPN to give the false impression that the user was located in a different jurisdiction, even though Binance would know that the user was, in fact, located in the United States.

These users were so valuable to Binance that personnel were instructed not to off-board them. A member of Binance's VIP team wrote in December 2020 that, "we will not be restricting the top 100 [users] (even after sending them emails [about restrictions applicable to U.S. users who remained on Binance.com]). They will be managed by your [VIP] team. [The CEO's] idea is that they should have enough time to create or find new non-US entities." Binance then executed the plan it had discussed, and it took additional steps to conceal its retention of U.S. users.

a. Binance Encouraged Customers to Alter KYC Documentation to Hide U.S. Nexus

Binance decided to first focus on the 22 most active U.S VIP users (in the highest tiers of Binance's VIP program). Binance's CEO described the goal of this exercise as "reduc[ing] the losses to ourselves, and, at the same time, to make the US regulatory authorities not trouble us." In furtherance of this goal, Binance's CEO inquired of Binance personnel about the process of getting new KYC documents for this subset of U.S. VIP users that would reflect an offshore entity: "[w]hat is the procedure for us to change KYC now," to which a senior Binance manager responded that "[w]e just change it directly. Just get in touch privately. Only 22 people! We just handle it case by case and do it off-line! There is no work order record." Similarly, when a VIP U.S. user struggled with changing his company's registration because the owner held a U.S.

passport, the former Chief Compliance Officer replied "[c]an he have someone else submit the entry and use a NON-U.S. passport[?]"[24] The CEO was updated on the status of these efforts.

b. *Binance Encouraged Customers to Access Binance from a VPN to Hide U.S. Activity*

Binance's CEO endorsed Binance's approach to handling VIP U.S. users that hadn't already completed KYC. Binance personnel had a special "script" for outreach to these U.S. VIP users wherein VIP personnel were instructed to "encourage user to create a new account on [Binance].com." Because such users had likely been identified as a U.S. person based on their IP address, the script further instructs VIP personnel "if the user doesn't get the hint, indicate that IP is the **sole** reason why he/she can't use .com."[25] Some Binance personnel used fake names when contacting customers because they were concerned about the process leaking and subsequently facing public pressure to be fired by the company.

Binance's former Chief Compliance Officer reiterated Binance's approach in February 2020, writing to another Binance employee that "we try to ask our US users to use VPN / or ask them to provide (if [they] are an entity) non-US documents / On the surface we cannot be seen to have US users but in reality, we should get them through other creative means." Similarly, in a December 2020 chat, Binance personnel discussed the issue of applying IP address controls to VIP users who access Binance.com via API: "VIP team wants to give [its users] temporary whitelist in a short time," notwithstanding the fact that such whitelisting "has regulatory risk also, because it will be seen that we are 'allowing' US ip [addresse]s."

[24] Binance had the same Chief Compliance Officer until early 2022.

[25] Emphasis in original. The former Chief Compliance Officer separately encouraged Binance personnel to offer VIP users "special treatment" and extra instruction to ensure they understood how to use VPNs.

c. Binance Attempted to Conceal the Retention of U.S. VIP Users

While Binance's VIP team facilitated the retention of U.S. users, senior management obscured Binance's ties to U.S. users by changing internal reports. Specifically, starting in January 2020, internal reports prepared by Binance's finance department included a breakdown of users associated with various countries, identifying a substantial portion in the United States. By late 2020, a senior manager instructed the employee in charge of Binance's internal database to reclassify the country code from "U.S." to "UNKWN" and to restrict access to view information about these users within the company. The following month's report from Binance's finance department shows that the change was implemented, with the United States no longer appearing on the country breakout and roughly the same proportion of users previously identified as U.S. users now marked as "UNKNWN."

Binance's CEO also told an employee "[d]on't post . . . U.S. data" in an internal group chat and instructed him to delete the message from the chat around the same time. In a contemporaneous October 2020 chat, a member of the VIP team informed the CEO that he was certain that a U.S. trading firm was "normally accessing the [Binance.com] api for trading via [U.S. technology vendor] Tokyo," to which the CEO replied "[g]ive them a heads up to ensure they don't connect from a us IP [address]. Don't leave anything in writing."

d. Specific VIP Users

The following examples further illustrate the lengths that Binance personnel have gone in order to maintain U.S. VIP users—despite supposed contemporaneous improvements in their KYC and AML compliance programs. Binance first purported to focus on the Enterprise User's beneficial owners as a primary indicator for whether an entity was a U.S. user. In 2022, Binance changed how it defined U.S. users, as the prior definition would require the offboarding of

commercially significant VIP users. Binance then purported to rely on a different test to determine whether an Enterprise User is a U.S. user, although as explained in the examples below, Binance continued to allow VIP users with material, commercially relevant ties to the U.S. to remain on Binance.com. Although Binance offboarded certain users by applying the revised test, during the Relevant Time Period, Binance never fully implemented these standards and retained U.S. VIP users on Binance.com through deliberate actions by Binance personnel to keep these users on the platform, vacillating between allowing U.S. VIP users to circumvent geofencing controls and changing the definition of a U.S. user altogether to justify the continued presence of U.S. VIP users with clear U.S. touchpoints. Binance agreed to begin taking steps to identify and offboard additional users following extensive discussions with FinCEN regarding Binance's continued retention of U.S. VIP users.

i. *Customer A*

Customer A first opened its account on Binance.com in January 2018, and from inception, Binance's records identified it as a U.S. user, but it appears that Customer A's activity on Binance was never restricted in any way. Customer A is a subsidiary of a well-known, U.S.-based trading firm that operates as the firm's CVC-focused subsidiary. This identification of Customer A as a U.S. user was consistent with U.S. indicia in documentation provided by Customer A during its initial registration and ample publicly available information showing that Customer A's majority beneficial owner is a U.S. citizen (Individual A-1).

Both Customer A and its parent are well known leaders in providing liquidity, and an affiliate of Customer A is registered with FinCEN as an MSB. Its registration notes that it engages in money transmission within the United States. Customer A's January 2018 account opening materials provided to Binance clearly identify its U.S. ties: the company's "Country and Territory"

field is listed as "USA," Customer A attached a photo of a U.S. passport for a Customer A employee, and an organization chart clearly identified Individual A-1 as Customer A's majority, ultimate beneficial owner. These materials were emailed to Binance's CEO and other Binance personnel.[26]

Numerous Binance reports identify Customer A as one of the top 10 overall spot market makers and liquidity providers on the Binance.com platform. Beginning in October 2019, Customer A began receiving "Market Maker Program" (sometimes referred to as "Spot Liquidity Provider Program") reports from Binance personnel, which depicted Customer A's relative spot trading activity in various CVC pairs on the Binance.com platform. These reports reflected the overall importance of Customer A's business to Binance. These reports also showed an uptick in Customer A's activity in the latter part of 2021, a trend that should not have occurred if Customer A was subject to the geofencing controls Binance purported to implement.

Despite Customer A's readily apparent U.S. indicia, Binance failed to take action with respect to its presence on the Biannce.com platform. In fact, Binance never allowed Customer A's trading to be affected by its geofencing controls; rather, Binance instructed Customer A on how to circumvent any such controls and designed them to not apply to users like Customer A. In September 2020, a member of Binance's corporate KYC team emailed Customer A personnel requesting, among other documents, "statutory documents of business registry for [Customer A's Cayman Islands subsidiary] ***reflecting the latest registered address instead***." Customer A personnel responded by providing a registered address for the subsidiary in the Cayman Islands,

[26] In the summer of 2019, Customer A personnel opened an account at Binance in the name of a Cayman Islands subsidiary that took over Customer A's trading on Binance. This subsidiary maintained a significant presence in, and reliance on, the United States through its parent.

despite Binance's records reflecting information indicating that Customer A was a U.S. user since January 2018.

In October 2020, a Binance employee wrote to Binance's former Chief Compliance Officer requesting for Customer A an "exemption of the US Nexus and passport copy for the [ultimate beneficial owner]" requirement. The former Chief Compliance Officer responded that "the Bitmex incident has made management more cautious of U.S. nexus . . . . can you please forward this message of mine to the biz team to see if they still want to proceed forward. If they still want to, I will exceptionally approve."[27] The former Chief Compliance Officer provided the approval that same day.

Throughout the Relevant Time Period, Binance never offboarded Customer A. Binance instead granted Customer A several additional extensions and attributed the delays in offboarding to the fact that Customer A is "a big client." In late 2021, rather than offboarding Customer A entirely, Binance transferred all of Customer A's "fee tiers, referrals, mm programs, etc.," to a "new" entity Customer A registered in the British Virgin Islands (BVI). Like Customer A, the BVI registered entity maintains, through its U.S. affiliates, a material presence in, and reliance on, the United States,[28] and continued to trade on the Binance.com platform, despite the fact that the

[27] In October 2020, the Commodity Futures Trading Commission (CFTC) charged the CVC exchange BitMEX with operating an unregistered trading platform and violating several CFTC regulations, including those related to AML. In August 2021, both the CFTC and FinCEN reached a consent resolution with BitMEX, with BitMEX's resolution with FinCEN resolving violations of BitMEX's willful failures to implement a Customer Identification Program, an AML program, and to file SARs. Commodity Futures Trading Commission, *CFTC v. HDR Global Trading Limited, et al.,* Complaint for Injunctive and Other Equitable Relief and Civil monetary Penalties Under the Commodity Exchange Act and Commission Regulations (Civil Action No. 20-cv-8132), (Oct. 1, 2020); Financial Crimes Enforcement Network, *In the Matter of HDR Global Trading Limited et al.* Assessment of Civil Money Penalty (Number 2021-02), (Aug. 10, 2021). https://www.fincen.gov/sites/default/files/enforcement_action/2021-08-10/Assessment_BITMEX_508_FINAL.pdf.

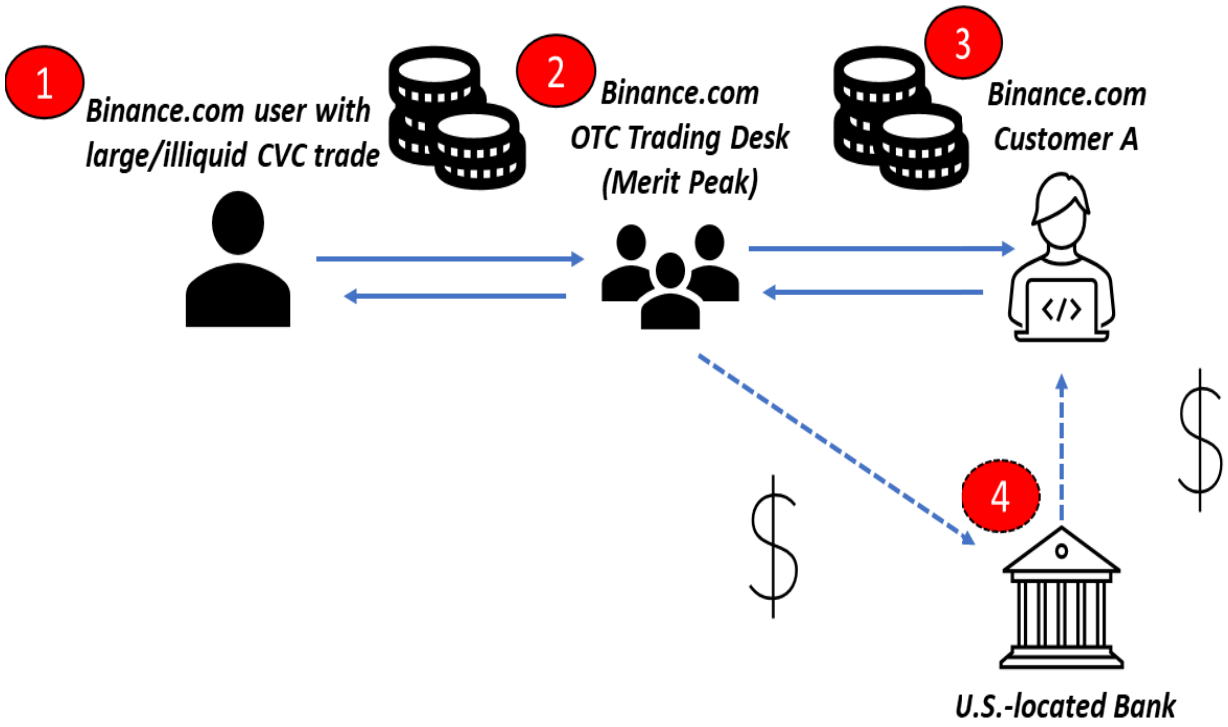
[28] Examples of the BVI entity's U.S. ties include, but are not limited to: (i) U.S. personnel are involved in the research, development, and testing of the algorithmic trading strategies that it employs; (ii) U.S. personnel provide some of the risk management, treasury, and operational services used by this entity; (iii) all of its UBOs are U.S. citizens; and (iv) on a monthly basis, a portion of its trading profits are transferred to a subsidiary of the U.S. parent entity.

opening of the new account violated Binance's contemporaneous Corporate Onboarding Procedure.[29] Binance offboarded Customer A in connection with the application of enhanced policies, procedures, and internal controls used to identify and offboard U.S. users that Binance implemented as part of its resolution with FinCEN.

aa. *Customer A's Relationship with Merit Peak*

In addition to Customer A's role as a market maker and liquidity provider on the Binance.com platform, Customer A was also an important trading counterparty to Merit Peak. As explained above, Merit Peak is one of the legal entities involved in Binance.com's operations, specifically by acting as Binance.com's OTC trading desk. In this capacity, Merit Peak would fill orders from Binance.com users for CVC trades that could not, or were not well suited to, be executed by Binance.com's order matching book (*e.g.*, trades of large order sizes or involving illiquid CVC pairs). However, Merit Peak described itself in documents provided to Customer A as a "proprietary trading firm with no client funds" that was "100% owned by [Binance's CEO]." In its capacity as Binance.com's OTC trading desk, Merit Peak executed numerous large CVC trades by accepting them from Binance.com customers and submitting corresponding CVC orders to Customer A for execution. As depicted in the diagram below, Binance.com was able to benefit from the U.S. liquidity that Customer A provided through both the Binance.com order book and OTC trades that Merit Peak entered into in a principal capacity to facilitate Binance.com trading.

[29] Binance's March 2022 Corporate Onboarding Procedure includes an illustrative example that is very similar to the BVI entity's corporate structure: a US parent company with an offshore subsidiary in an offshore jurisdiction (in the example, it is the Cayman Islands). However, the example from Binance's procedure is beneficially owned by five persons with an equal stake (*i.e.*, 20% each), only one of whom is a U.S. person. The example concludes that it would be acceptable to onboard such an entity because it did not hit any of three prohibited criteria, one of which is listed as "total shareholding of the UBOs has 50% or more in a restricted jurisdiction." Accordingly, Binance's contemporaneous procedures indicate that an entity like Customer A and its BVI affiliate, which is more than 50% beneficially owned by a U.S. person, should not have been allowed to open or maintain an account on the Binance.com platform.



1. *Binance.com user wishing to execute a large or illiquid CVC trade places an order with Binance.com's OTC trading desk (Merit Peak)*
2. *Binance.com's OTC Trading Desk (Merit Peak) accepts the order and finds a trading firm—often one of Binance's VIP users—to send the order for fulfillment*
3. *In this example, Customer A accepts Merit Peak's order and buys or sells CVC to fulfill it*
4. *If the trade is CVC-to-CVC, it settles entirely within Binance.com. If the trades is CVC-to-USD, the CVC would settle within Binance.com, and Customer A and Merit Peak would settle the USD through a U.S.-located bank.*

Between April 2019, when Merit Peak entered into an agreement with an affiliate of Customer A, and September 2021, when Customer A and its affiliates ceased trading with Merit Peak, Customer A effected roughly $1.2 billion in CVC transactions with Merit Peak. The CVC portion of these trades settled through Customer A's account on the Binance.com platform. In connection with one such trade, Merit Peak made a statement to Customer A personnel about Binance's concerns regarding compliance with U.S. regulations: "we [Merit Peak] can't use usd pair [to trade with Customer A] since there's no way to settle usd on [Binance].com. . .there's

certain legal risk we gonna face if we put USD on our website." However, as depicted in the graphic above, subsequent confirmations of trades between Customer A and Merit Peak indicated that trades were effected in USD pairs, with the USD settling through a Merit Peak account at a U.S. financial institution.

ii. *Customer B*

Customer B became a customer of Binance in May 2018, and Binance sent to Customer B a form communication used with other VIP users that referred to Customer B as one of its "most treasured VIP customers." Customer B was a privately held, U.S.-based CVC trading firm and Cayman Islands-incorporated subsidiary of a Chicago-based trading firm. Throughout the period in which it maintained an account on Binance.com, Customer B maintained a presence in, and reliance on, the United States[30] and would use a VPN to access its Binance.com account from the United States. As with Customer A, an affiliate of Customer B maintains an MSB registration with FinCEN. Customer B maintained accounts on both Binance.com and Binance.us.

Despite obvious U.S. indicia—both publicly available and within Binance's own records—Binance failed to offboard or restrict Customer B's account in a manner consistent with Binance's purported geofencing controls until late 2022, well after Binance purported to have implemented enhanced controls to identify and offboard U.S. users. Additionally, in June 2019, a Customer B employee specifically asked in a chat with Binance personnel "[h]ey guys, will our account be affected by the new Terms of Service[?] We registered through our Cayman entity," to which a member of Binance's VIP team responded, "***[y]ou will continue to have access to [Binance].com[.] Amendments to the terms of use apply to the us based entities***." Indeed,

[30] Examples of Customer B's U.S. ties included, but were not limited to: (i) U.S. personnel researched, developed, and tested the trading strategies it employed, (ii) U.S. personnel managed and oversaw its trading functions, (iii) U.S. personnel provided other services to support its operations, and (iv) a substantial majority of Customer B was owned by two U.S. individuals: Individual B-1, a Miami-based individual, and Individual B-2, a Chicago-based individual.

Binance never restricted any of Customer B's activities, even when Binance's automated IP address detection software logged locations suggesting the use of a VPN by Customer B to hide its U.S. nexus.

iii. *Binance Retained Numerous Exchange Brokers that Facilitated U.S. Trading*

In addition to Binance continuing to maintain commercially important U.S. trading firms on the Binance.com platform, Binance also maintained relationships with a variety of brokers. Specifically, these brokers generally fell into the following two categories:

- Brokers whose clients were able to access Binance.com, either through the broker's API or a referral to Binance placed on the broker's website via a "widget." Clients of these brokers were required to register with Binance.com and were subject to Binance's KYC/customer due diligence controls.
- So-called "Exchange Brokers,"[31] whose clients were allowed to trade on Binance.com via sub-accounts under the broker's Binance.com account. Exchange Brokers clients' orders were filled through the Binance.com order book and therefore used the Binance.com platform to effect transactions, ***but such clients were not required to register with Binance.com***. Exchange brokers were able to operate in this manner because of Binance's former policy allowing any entity registered with Binance.com as an Exchange Broker to open an unlimited number of sub-accounts, which existed on *Binance's* platform, with "***no requirement for extensive verification of sub-account users.***"[32] In recognition of the minimal oversight that Binance maintained over these Exchange Brokers, Binance's

[31] Later in the Relevant Time Period, Binance began referring to such users as "Link Brokers."

[32] The AML Program section of this Consent Order describes the implications of this policy on Binance's ability to effectively manage its money laundering and terrorist financing risks. *See* Section II.E.3, *infra*.

relevant procedures described them as "operat[ing] their own exchange" within Binance.com.

Binance personnel actively recruited brokers, including Exchange Brokers, to its platform. For example, in a December 2020 chat, Binance personnel discussed an upcoming presentation which noted that the broker program had onboarded hundreds of brokers in more than 40 countries and that this program generated millions of dollars per month for these brokers. Similarly, in a collection of Binance's marketing team's "objectives and key results" (referred to as "OKRs"), an employee on the "user operation" team wrote that his objectives included "an average of 400 new customers per day at the end of the year" through the "brokerage broker project," and that, to help achieve a target average monthly exchange volume, "at least 30 new brokers will be connected by the end of the year."

Binance maintained effectively no geofencing or AML controls over the broker program until late 2021 (*i.e.*, well after geofencing controls applicable to other Binance.com customers went into effect). Consistent with its overall approach to geofencing, its initial controls were ineffective and, until Binance made certain, recent changes in connection with the resolution of FinCEN's investigation, remained inadequate. In September 2021, Binance began to update the licensing agreement that Binance required its Exchange Brokers to sign. This update included a new clause containing representations regarding the Exchange Broker's AML and KYC controls. However, Exchange Brokers were not required to agree to the revised version of this agreement until the end of 2021.

Moreover, Binance did not begin to take steps to independently evaluate an Exchange Broker's KYC and AML controls until 2022. Prior to 2022, Binance's corporate onboarding procedures did not include any requirement to review an Exchange Broker's AML controls.

Although a March 2022 version of Binance's corporate customer onboarding procedure document includes a section specifically dedicated to Exchange Brokers, it contains no reference to any requirement that Binance personnel review geofencing controls or policies related to U.S. persons. Once Binance actually began to evaluate Exchange Brokers' controls, many ultimately offboarded from the platform.

As of November 2022, Binance maintained relationships with roughly 100 Exchange Brokers. A detailed review of roughly half of these brokers indicates that, based on publicly available information, 6 are U.S. firms, 16 exhibited clear indicia of serving U.S. users, and 22 brokers appeared not to impose any restrictions applicable to U.S. users. Notwithstanding Binance's assertion that it has implemented enhanced controls applicable to Exchange Brokers, Binance.com continued to do business with brokers that:

- advertise offering "simplified KYC" for Binance and that they did not require "complex registration procedures;"
- in the case of one broker, described by a third-party website as "welcome[ing] . . . traders in United States;" and
- in the case of another, Russian broker, allow users to create an "exchange account" by providing only an email address, a practice that mirrors Binance's "Tier One" (no-KYC) accounts described below that it purported to prohibit starting in August 2021.

In connection with Binance's resolution with FinCEN, Binance agreed to cease its practice of opening anonymous sub-accounts and permitting them to transact on or through Binance.com.

iv. *Customer (Exchange Broker) C*

Customer C, a BVI entity, was founded by Individual C-1, who previously worked at a well-known Connecticut-based hedge fund. Customer C's primary business model appears to be

allowing trading firms and other institutional market participants to access various CVC exchanges through Customer's C platform. By having their orders consolidated with those of other Customer C clients, trading firms and other institutional market participants receive lower fees and better rebates from the various CVC exchanges at which Customer C maintains accounts. Customer C is one of Binance's largest customers. For example, as-of late May 2022, Customer C's total transaction activity represented roughly 3.2% of all spot trading activity on the Binance.com platform.

For much of the Relevant Time Period, Customer C did not maintain a publicly accessible website, but was controlled, indirectly, by a U.S.-organized limited partnership that has filed Form D notices with the SEC identifying Individual C-1 as the manager of its general partner and lists a New York address for Individual C-1. In addition to Individual C-1's role as manager of the partnership, key personnel of Customer C publicly identify themselves as being based in the United States. A Customer C affiliate also maintains a futures commission merchant registration with the CFTC and National Futures Association.

Beyond Customer C's public connections to the United States, Customer C also discussed with Binance personnel Individual C-1's status as a U.S. person. In a May 2021 email thread about completing onboarding on the Binance.com platform, Customer C's General Counsel asked a member of Binance's VIP team if there was "any concern with a non-US domiciled corporate vehicle having a US domiciled director." The Binance employee appears to have called Customer C's General Counsel instead of replying by email. After this discussion, Customer C's General Counsel wrote to another member of Binance's VIP team tasked with KYC onboarding and reported that Customer C could not "input anything on [Individual C-1] since it won't let me choose USA as a place for his passport." This Binance employee replied, "***you can select any***

other country (Cayman Islands per example) and input his selfie and passport." Finally, in January 2022, Customer C reported connectivity issues to Binance personnel, and, in doing so, referenced IP addresses that FinCEN identified through open-source research as being located in the United States.

In addition to Customer C's own U.S. ties, more than twenty percent of Customer C's trading firm clients exhibit U.S. indicia. Binance should have been aware of this, as it sought "to regularly review [Customer C's] client list and keep onboarding of new clients as transparent as possible" for Binance's record and risk management purposes. Customer C also referenced a high-profile U.S. trading firm as one of its clients in communications with Binance personnel, and Binance provided technical support for another U.S.-based Customer C client, stating "seeing [that] it's a US entity, API specifications may differ."

v. *Customer (Exchange Broker) D*[33] *and Customer E*

Customer D is an Exchange Broker customer of Binance with a material presence in, and reliance on, the U.S. A Customer D affiliate is registered with FinCEN as a money transmitter with activity occurring throughout the United States and territories. Another Customer D affiliate is provisionally registered with the CFTC as a swap dealer and is a member of the National Futures Association. Customer D offers a "prime service" that is similar to Customer C's main offering: It allows trading firms to access multiple CVC exchanges under Customer D's account on those exchanges via Customer D's user interface. A significant portion of Customer D's customers are U.S. trading firms and other institutional market participants. Customer D's subaccounts on Binance.com for these U.S. firms demonstrate that Binance's geofencing controls—even though

[33] The following description of Customer D is applicable to the majority of the Relevant Time Period. Customer D recently began to adopt remedial measures to limit its own presence in, and reliance on, the U.S., as well as to identify and offboard its U.S. clients, including Customer E.

they evolved over time—remained ineffective and that, notwithstanding its representations to the contrary, Binance was not ringfenced from the United States.

One of Customer D's U.S. customers is Customer E. Customer E is an affiliate of a U.S.-based trading firm. Through its U.S. affiliates, Customer E maintains a material presence in, and reliance on, the United States.[34] Customer E became a client of Customer D in order to evade improvements in Binance KYC that limited its ability to continue trading on the Binance platform. When onboarding, Customer D wrote to Customer E, "***[Customer E] wouldn't have to KYC with the exchange, we could do the KYC on our side—you could connect via API and be under the Customer D subaccount***."

This move occurred after Customer E had already changed its KYC with Binance.com three times to avoid regulatory requirements associated with doing business in the United States and other countries. The first registration change occurred in June 2019 in response to Binance's press announcement that it would stop serving U.S. traders on the Binance.com platform. A member of Binance's VIP team assured Customer E that it would "***help to transfer the VIP level and withdrawal limits and API order limits and other settings***" from the existing account to Customer E's "new" account. The Binance VIP team employee encouraged Customer E to evade Binance's geofencing controls by stating that "***you need to use VPN when you open the registration link, make sure not a US IP address.***" After onboarding with Customer D, Customer E has proceeded with its business just as it had under all the various prior registrations facilitated by Binance.

[34] Examples of Customer E's U.S. ties include, but are not limited to: (i) a clear majority of key personnel are based in the United States; (ii) technology, intellectual property (including the development of trading algorithms), and trade support are provided by the U.S. affiliate; and (iii) the U.S. affiliate indirectly provides Customer E's capitalization, and, in exchange, Customer E pays net profits back to the U.S. affiliate.

4. *Binance's Launch of a "U.S." Entity Was Intended to Shift Regulatory Focus and Did Not Result in Binance Exiting the United States*

In the fall of 2018, Binance senior management, received two presentations (referred to within Binance, and herein, as the "Tai Chi Presentations") on how to address issues related to the U.S. market, which discussed ways that Binance could avoid scrutiny from U.S. authorities. Specifically, one of the Tai Chi Presentations stated that the U.S. entity would use "explicit Binance branding to attract regulatory and enforcement attention" and then "accept nominal fines in exchange for enforcement forbearance" on Binance's behalf. The presentation noted that, in doing so, the U.S. entity would "become the target of all built-up enforcement actions" and therefore "insulate Binance." In effect, the U.S. entity would serve as a decoy to distract from Binance's continued U.S. presence, which it would achieve in part by instructing U.S. users on how to evade geofencing controls on Binance.com, as explained above, and by having U.S. users maintain accounts on both Binance.com and Binance.us. Although Binance's senior management sent the author of the Tai Chi presentation a message rejecting the presentations' approach, Binance's actions following these presentations demonstrate Binance's aim in establishing the Binance.us entity as a vehicle to distract U.S. authorities from Binance.com's continued U.S. presence while simultaneously increasing Binance's U.S. footprint.

First, as explained above, Binance.com took deliberate steps to continue (but obscure) its relationships with U.S. trading firms after the launch of Binance.us, despite Binance's public and private assertions to the contrary. Leading up to the launch of Binance.us, Binance.us's CEO was assured that Binance would start blocking U.S. users on Binance.com after Binance.us obtained its MSB registration from FinCEN. However, Binance.com did not begin blocking U.S. users after Binance.us obtained its MSB registration from FinCEN. As explained above, the implementation of geofencing controls—which were the primary measures Binance took to try to

block U.S. users on the Binance.com platform—was incremental, protracted, and ineffective. Moreover, Binance instructed its personnel to offer U.S. trading firms the possibility of continued, improper retention of accounts on Binance.com in return for a commitment from those firms to increase their activity on Binance.us.[35] This approach was entirely consistent with portions of the Tai Chi Presentations, which specifically contemplated methods to allow U.S. trading firms to play a role on *both* Binance.com and Binance.us.

Second, correspondence between Binance senior management indicate that certain of them endorsed the Tai Chi Presentations and understood the import. After launching Binance.us, Binance's former Chief Compliance Officer wrote to Binance's then-CFO:[36] "Our downside now is we cannot acknowledge US presence (even historical) on [Binance].com . . . If US reg[ulator]s want to hit you for [Binance].com's sins of the past, guess what[?] you have a direct avenue in BAM [Binance.us] for them to reach/hammer you." The then-CFO responded, "***[t]hat was one of the purposes of having BAM in place.***"

Third, Binance.us has generally lacked autonomy from Binance in two key respects: (i) Binance.us is dependent on Binance for several business-critical services, including the provision of wallet software services, as well as various IT and software-related services (such as Binance.us's reliance on Binance.com's matching engine, risk control center, and Android/iOS mobile applications to operate);[37] and (ii) Binance.us's board of directors has always consisted of

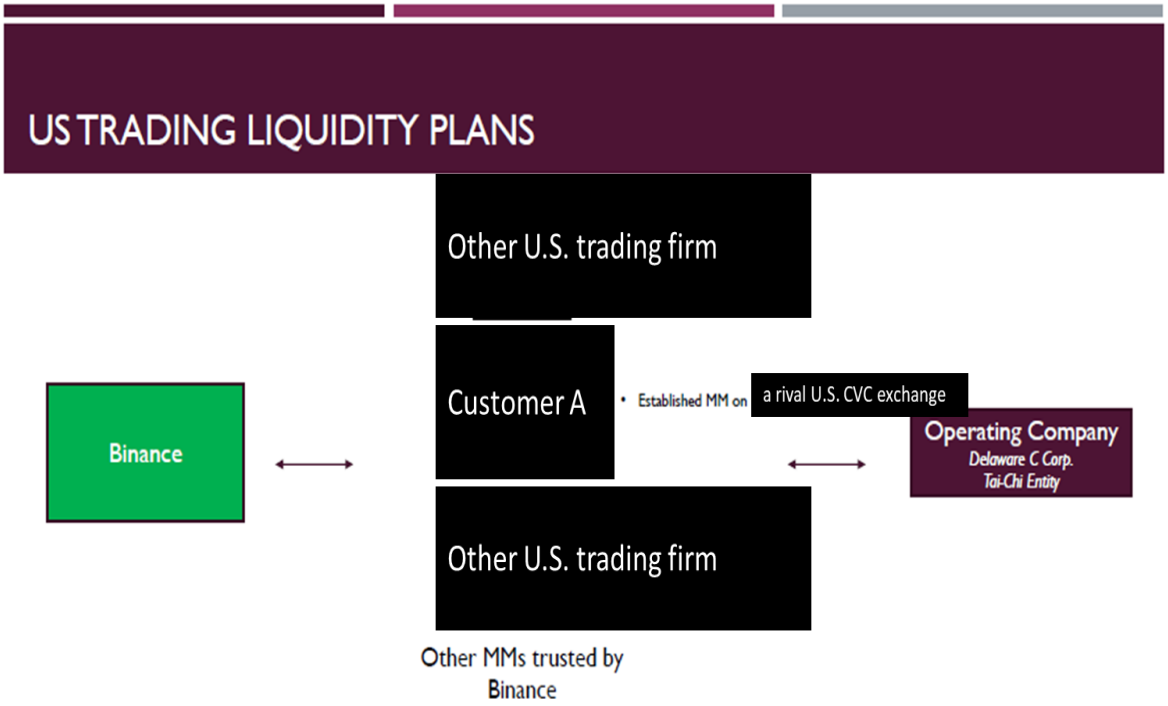
[35] See Section II.D.3, *infra*.

[36] Binance's then-CFO also served as one of the directors of BAM for part of the Relevant Time Period.

[37] For a substantial portion of the Relevant Time Period, Binance.us personnel were unable to access key data about Binance.us's own operations without going through Binance.com personnel based in China, even when that data was needed to respond to U.S. regulatory requests.

only three individuals: Binance.us's CEO, the CEO of Binance.com, and a third director affiliated with Binance.com.[38]

This lack of independence allowed Binance's CEO to use Binance.us to facilitate activity of his proprietary trading firms: Sigma Chain AG (Sigma Chain) and Merit Peak Limited (Merit Peak).[39] Moreover, because Merit Peak also functioned as Binance.com's over-the-counter (OTC) trading desk, Merit Peak was able to use Binance.us as a way for Binance.com to continue to access the U.S. CVC market. In fact, this approach is entirely consistent with the Tai Chi Presentations: as indicated in the below excerpt, one of the presentations described a structure in which shared market makers would provide liquidity on both Binance.com and Binance.us, with Customer A specifically identified on this slide as one of the firms expected to act in this capacity.



[38] On several occasions, BAM's former CEO requested that the size of its board of directors be expanded. Although the former CEO received assurances that a change in BAM's board size and composition was being contemplated, these changes were never implemented.

[39] Both Merit Peak and Sigma Chain are wholly-owned by Binance's CEO.

Merit Peak supported this arrangement and contributed to Binance's operations as an unregistered MSB in two principal capacities: (i) Merit Peak relied on Binance.us's settlement infrastructure and U.S. dollar liquidity to convert U.S. dollars into Binance's stablecoin (BUSD) on behalf of Sigma Chain, which acted as a market maker on Binance.us; and (ii) Merit Peak also facilitated OTC trades of CVC (including by sourcing CVC through Customer A, whose CVC trades would settle on Binance.com) for customers of Binance.us, despite the fact that Merit Peak, as a part of Binance.com, was not registered to provide such services to Binance.us users.

In effect, Merit Peak acted as a conduit between Binance.us and Binance.com, while exploiting Binance.us's corporate governance weaknesses to avoid scrutiny of this activity. Binance.us's own CEO was never given visibility into what compensation (if any) that Binance.us received for referring lucrative, OTC business to Merit Peak. Moreover, when Binance.us's CEO questioned several large withdrawals by Merit Peak from Binance.us, Binance.us never received information from Merit Peak or Binance to adequately explain either the purpose or the parties involved.

In sum, for most of the Relevant Time Period, Binance made no serious effort to eliminate U.S. activity from Binance.com, despite its contrary representations, and the creation of Binance.us did not result in a separate platform for all U.S. operations. Instead, Binance.us effectively provided cover for Binance.com's continued service of U.S. customers.

E. Failure to Develop, Implement, and Maintain an Effective AML Program

In addition to willfully failing to register as an MSB, Binance also during the Relevant Time Period willfully failed to develop, implement, and maintain an effective money laundering program reasonably designed to prevent it from being used to facilitate money laundering and the financing of terrorist activities. Binance launched its initial platform without any AML controls

in place, failing to establish a written AML program until July 2018—a year after Binance launched and well after the 90-day deadline required under FinCEN's regulations. Throughout the Relevant Time Period, Binance's AML program contained categorical gaps with respect to KYC and transactions in anonymity enhanced cryptocurrencies (AECs), as well as numerous other deficiencies, which rendered it ineffective.

1. *Binance's KYC "Tiers" Allowed Users to Trade without KYC*

MSBs are required to develop, implement, and maintain an effective AML program that includes policies, procedures, and internal controls for verifying customer identification.[40] Binance initially adopted a "tiered" approach to identifying and verifying customers. Binance characterized this as a risk-based approach, but in reality it resulted in a categorical gap in its policies, procedures, and internal controls. Most significantly, from July 2017 through at least August 2021, "Tier One" (also referred to as "no-KYC")[41] customers were permitted to open accounts and conduct CVC-to-CVC transactions with only an email address. Binance performed no due diligence on such accounts. "No KYC" account-holders were permitted to conduct daily withdrawals of CVC under two bitcoin, a value that at times exceeded the equivalent of $130,000 a day.[42] By Binance's own calculations, it had four times the number of U.S. users for whom Binance had not collected KYC (based on IP address) than U.S. users for whom Binance had conducted KYC.

Indeed, Binance was aware that such a practice was high-risk and constituted a willful failure to comply with the BSA and its implementing regulations. Shortly after Binance launched

[40] 31 C.F.R. § 1022.210(d)(1)(i)(A).

[41] Although Binance prohibited users from opening new no-KYC accounts starting in August 2021, it did not remediate the lack of KYC for pre-existing accounts until May 2022.

[42] Additionally, Binance extended this tiered approach to fiat transactions and permitted fiat withdrawals of up to $300 per day by "Tier One," no-KYC accounts.

in July 2017, FinCEN, in collaboration with U.S. law enforcement, brought enforcement actions against the Russian-located money transmitter BTC-e, which also permitted customers to trade without KYC.[43] Soon thereafter, Binance's third-party service provider briefed Binance's former Chief Compliance Officer on FinCEN's action and the parallels with Binance's practices.

Senior management at Binance were also aware that its "no KYC" accounts were being exploited by illicit actors on the Binance.com platform. In an August 14, 2018 email conversation, one of Binance's third-party service providers discussed with Binance's former Chief Compliance Officer a large movement of illicit funds. The service provider explained, "[w]e have been tracking some stolen money that is coming from one of the worst hacking groups we have seen (more than $130m in stolen funds). They seem to be using Binance as one of the cash out venues… There seems to be structuring occurring that is just under your KYC limit of 2 [bitcoin]…" Separately, a third-party service provider company told Binance in March 2019 that effective screening could not be performed without minimal information, including first and last name (as opposed to an email address). In other words, no sanctions screening could occur for "no KYC" accounts.

Despite these warnings from the third-party service providers—and subsequent escalation to senior management—Binance failed to address this significant compliance gap for over four years, when it finally began offboarding the "no KYC" accounts.

2. *Binance's Lack of KYC Led to a "Paper-only" AML Program*

An MSB must develop, implement, and maintain an effective AML program, which must be in writing and commensurate with the risks posed by the location, size and nature of the volume

[43]Financial Crimes Enforcement Network, *In the matter of BTC-e a/k/a Canton Business Corporation and Alexander Vinnik*, Assessment of Civil Money Penalty Number 2017-03, (July 27, 2017).

of financial services provided by the MSB.[44] When Binance finally drafted an AML program, roughly a year after its initial launch, it listed many practices that were either never fully implemented or were directly contradicted by Binance's own practices. For example, Binance's policies, procedures and internal controls specifically set out that Binance customers are prohibited from "opening accounts for or establish[ing] relationships" with potentially suspicious counterparties, including "online casinos and unlicensed casinos." This is also separately affirmed by Binance's written transaction monitoring procedures, which state that "gambling" platforms are a "high risk counterparty" that would be "identified and 'flagged'" through Binance's use of blockchain analytic tools.

However, Binance's policy of allowing users to open accounts without undergoing KYC meant that, in practice, Binance users were free to transact with these high-risk counterparties with impunity. A review of Binance's transactional history on multiple blockchain tools—some of which Binance purports to have utilized (albeit in only a limited capacity)—demonstrates that Binance has directly sent and received over $1 billion with known gambling services and online casinos during the Relevant Time Period.[45] Each of these financial institutions bore additional indicia that they were high-risk as well, as none of these identified counterparties are duly licensed as casinos or card clubs in the United States or registered as MSBs.

Similarly, following Russia's invasion of Ukraine in early 2022, Binance purported to focus on the risks associated with Russian illicit finance. However, FinCEN identified that Binance continued to have significant, ongoing exposure to Russian illicit finance. Examples of such connections included: (i) processing hundreds of millions of dollars in transactions for a CVC

[44] 31 C.F.R. § 1022.210(a)-(c).

[45] Binance first contracted with a blockchain analytics company in August 2018, over a year after it began business.

exchange co-owned by a Russian citizen who pled guilty to money laundering in February 2023, including transactions effected after this individual's guilty plea; (ii) processing several million dollars for a CVC exchange that allowed its users to "cash out" at a Russian bank designated by OFAC and that had substantial exposure to the Russian darknet market Hydra Market; and (iii) as recently as the summer of 2023, continuing to effect transactions with the darknet market Russia Market, one of the largest cybercrime service websites in the world.

The high volume of activity that Binance effected with online and unlicensed casinos as well as Binance's continued connections to Russian illicit finance despite intense public scrutiny of such activity indicates that Binance did not effectively implement its "paper" policies and procedures.

3. *Insufficient Policies, Procedures, and Internal Controls for Subaccounts and "Nested" Exchanges*

As noted above, an important source of Binance's growth and its ongoing, sustained success as the largest CVC exchange by trading volume has been its recruitment and retention of large trading firms, including Exchange Brokers. Binance allows Exchange Brokers' clients to directly access the Binance.com platform through subaccounts created by the broker under its own Binance.com account. However, Binance initially failed to implement adequate policies, procedures, and internal controls around these customer-opened subaccounts to ensure that the Binance.com platform was not exploited by illicit actors. In fact, Binance told Enterprise Users that this product had "no requirement for extensive verification of sub-account users" and that a single Enterprise User could open up to 1,000 subaccounts on the Binance.com platform under its master account. Exchange Brokers could open an unlimited number of subaccounts. In fact, until the end of 2021, Binance failed to require attestation from Exchange Brokers to confirm that these exchange brokers perform any AML checks on their own customers, including subaccount holders.

These subaccounts, in addition to Binance's "No KYC" accounts, contributed to the establishment of so-called "nested exchanges" operating within Binance without sufficient oversight and due diligence. Binance knew how nested exchanges operate and the challenges they create. According to Binance's own educational "Academy" webpage, a nested exchange "provides its customers with [CVC] trading servicers through an account on another exchange . . . . [I]t acts as a bridge between [Binance] users and other service providers."[46] Binance further describes this threat adding, "nested exchanges often have lax KYC and AML processes or none at all . . . [and] support money laundering, scammers, and ransomware payments." Despite this recognition by Binance itself, numerous nested exchanges operated without any controls on the Binance.com platform until at least 2021, including the nested exchanges described below that were eventually designated by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and shut down by law enforcement.

One such example was SUEX OTC, S.R.O. (Suex), a Russian CVC exchange which was designated on the Specially Designated Nationals and Blocked Persons (SDN) List maintained by OFAC in September 2021 for its role in facilitating transactions of illicit funds from numerous criminal schemes.[47] Suex processed transactions involving illicit activities ranging from ransomware attacks, including the Colonial Pipeline hack, to transactions involving the illegal CVC exchange BTC-e[48] through accounts held at Binance. The exchange operated on the

[46] Binance Academy, *What Are Nested Exchanges and Why Should You Avoid Them?* (Dec. 3, 2021, updated Jan. 14, 2022).

[47] U.S. Department of the Treasury, *Treasury Takes Robust Actions to Counter Ransomware*, (Sept. 21, 2021).

[48] Financial Crimes Enforcement Network, *In the matter of BTC-e a/k/a Canton Business Corporation and Alexander Vinnik*, Assessment of Civil Money Penalty Number 2017-03, (July 27, 2017)..

Binance.com platform through maintaining multiple non-KYC accounts, including subaccounts on the Binance.com platform that Suex itself opened, for years prior to its designation.

Additionally, OFAC-designated CVC exchange Garantex, had been operating as a nested exchange on Binance since its inception in March 2019 until one month before it was designated by OFAC.[49] A blockchain analytic tool, also utilized by Binance, identified close to 100,000 transfers between Garantex and Binance between March 2019 and 2022. Despite Garantex conducting over $100 million in potentially suspicious transactions with illicit actors, including $6 million associated with Conti ransomware, Binance's lack of KYC and other deficient controls allowed the service to operate on its platform for almost three years without Binance reporting any suspicious activity. Well after Garantex's designation by OFAC in April 2022, there were tens of millions of dollars in transactions with Garantex by Binance, extending into 2023.

Finally, BestMixer conducted illicit activity and obfuscated law enforcement investigations,[50] and used Binance's "No-KYC" accounts—which remained in place for the majority of the Relevant Time Period—to achieve its objectives. BestMixer utilized multiple unique accounts on the Binance platform and conducted thousands of transactions between 1.9 and 2 bitcoin—just below, or at, the limit of Binance's "No-KYC" policy. Through splitting bitcoin between different Binance accounts to remain below Binance's two bitcoin withdrawal limit, this "mixer"[51] was able to send over $40 million in bitcoin by structuring transactions based on Binance's "No-KYC" threshold. After the service was taken down by law enforcement, a

[49] *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex*, U.S. Department of the Treasury (Apr. 5, 2022).

[50] *Multi-million euro cryptocurrency laundering service Bestmixer.io taken down*, EUROPOL (May 22, 2019).

[51] "Mixers" or "tumblers," accept CVCs and retransmit them in a manner designed to prevent others from tracing the transmission back to its source. *See* Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001, (May 9, 2019).

blockchain analytic tool company that was also a third-party service provider to Binance, informed Binance that "[B]estmixer [h]ave been consistently using Binance as a source of 'clean' coins."

Despite this information, Binance failed to implement any changes to its policies and procedures on nested exchanges and allowed multiple nested exchanges to continue to operate on the platform without appropriate restrictions or oversight. In connection with its resolution with FinCEN, Binance agreed to cease the practice of opening anonymous sub-accounts and allowing them to transact on or through Binance.com.

4. *Insufficient Policies, Procedures, and Internal Controls Around AECs*

Throughout the Relevant Time Period, Binance continued to operate without appropriate procedures to manage the risks associated with its various products and services. Most significantly, that includes risks associated with AECs. AECs use various approaches to hide the sender and/or recipient addresses associated with a CVC transaction and therefore pose heightened money laundering and terrorist finance risks, particularly when VASPs that offer AECs to their customers fail to implement mitigating controls specifically tailored to these products. During the Relevant Time Period, Binance offered at least six of the most popular AECs by market share, including the most popular one, monero.[52] To date, Binance processes almost double the volume of transactions in monero relative to the next closest CVC exchange that transacts in it—without

[52] Monero's protocol includes features that prevent tracking by using advanced programming to purposefully insert false information into every transaction on its private blockchain. The false information is impossible to separate from the valid payment details, effectively concealing sender data and completely hiding all transaction amounts. The Monero network ultimately sends funds to an auto-generated, one time use only, wallet known only to the transacting parties. It is designed to make supervisory transaction monitoring virtually impossible. Moreover, wallet addresses on Monero's private blockchain are selectively visible only when an observer has obtained a private "view key." *See* The Monero Project, Moneropedia: View Key (last visited Sept. 13, 2023).

policies, procedures, or controls designed to mitigate the inherent AML/CFT risk associated with AECs.

Binance's failure to implement controls around the specific risks associated with its products and services left it unable to comply with its AML program obligations or its obligation to identify and report suspicious activity occurring on its platform. This, coupled with Binance's "No-KYC" policy hamstrung reporting critical to law enforcement efforts. In connection with its resolution with FinCEN, Binance began undertaking remedial measures to mitigate this risk, including: (i) delisting some of the highest volume AECs—including monero—from trading on Binance.com and restricting deposits and withdrawals in these AECs by Binance users, and (ii) prohibiting listing, and restricting deposits and withdrawals, of other AECs that are either fully private, or are partially private and that lack sufficient policies, procedures, and internal controls to mitigate the associated illicit finance risks.

5. *Insufficient Policies, Procedures, and Internal Controls for Responding to Law Enforcement Requests*

As an MSB operating during the Relevant Time Period, Binance was required to implement policies, procedures, and internal controls to respond to law enforcement requests.[53] Binance failed to implement a formal policy to respond to law enforcement requests until 2020. Even then, Binance initially imposed improper restrictions on U.S. law enforcement's access to information. Rather than comply with subpoenas issued by law enforcement agencies, Binance tried for years to force U.S. law enforcement agents to first sign statements that would "indemnify and hold harmless Binance . . . from and against any regulatory or legal action, financial losses, liabilities, costs (including reasonable attorneys' fees)." Processes that effectively deny, or delay, U.S. law

[53] 31 C.F.R. § 1022.210(d)(1)(i)(D) (mandating that such policies, procedures and internal controls include "[r]esponding to law enforcement requests").

enforcement and regulators access to information required to be available by law are incompatible with an effective AML policy. Yet, Binance codified this policy of withholding crucial information from U.S. law enforcement without indemnification through at least August 2021.

6. *Insufficient Policies, Procedures, and Internal Controls for High-Risk Jurisdictions*

Binance's policies, procedures, and internal controls around the location of its customers were critically deficient, as reflected by its geofencing controls. Binance's geofencing not only allowed U.S. users to access the platform (as described above), but also allowed users from high-risk jurisdictions to access the platform without appropriate controls. Binance personnel were aware that its poor geofencing controls meant that users from jurisdictions designated by Financial Action Task Force (FATF) on the grey or blacklist[54] or subject to comprehensive sanctions could access the platform; this also meant that Binance's AML controls would not be sufficient to meet its SAR obligations.

For example, in April 2020, a company with which Binance wanted to partner expressed concern that, "as part of the due diligence process, [our] Compliance team was able to open accounts with an . . . Iranian address on Binance.com. The Iranian test was opened using an Iranian IP and an Iranian address." This was far from an isolated incident, as by Binance's own estimates, between June 2017 and September 2021, Binance processed over 1,000,000 transactions with an aggregate value in excess of $500 million between U.S. users and users accessing the platform via an Iranian IP address. FinCEN has repeatedly highlighted risks associated with transactions with

[54] FATF's "grey list" refers to countries under increased monitoring; FATF's "black list" consists of high-risk jurisdictions subject to a call for action. *See* Financial Action Task Force, *"Black and grey" lists* (last visited on Sept. 13, 2023).

Iran[55] and named Iran a jurisdiction of "primary money laundering concern" in a rulemaking finalized in 2019.[56]

7. *Binance's Failure to Designate a Person to Assure Day-to-Day Compliance with the BSA*

As an MSB, Binance was required to designate a person to assure day to day compliance with their AML program and the BSA.[57] Binance failed to designate a person to handle AML compliance until it hired its first Chief Compliance Officer in April of 2018—nearly a year after launch. However, given the size and complexity of Binance's operations, as well as the high-risk nature of many of its activities, this individual was not qualified for the role. Specifically, he lacked knowledge of AML/CFT obligations and had little-to-no experience designing and overseeing an AML/CFT compliance program. Moreover, the former Chief Compliance Officer actively participated in the development and execution of the strategy to conceal Binance's efforts to unlawfully serve U.S. customers without registering as an MSB. The former Chief Compliance Officer was specifically briefed on the implications of failing to register with FinCEN and comply with the BSA.

8. *Binance's Failure to Provide Education or Training of Appropriate Personnel*

Binance was required to provide education and/or training of appropriate personnel concerning their responsibilities under the AML program including training in the detection of suspicious transactions.[58] Binance did not provide sufficient training on the detection of potentially suspicious transactions and employee obligations under the AML program. Binance

[55] Financial Crimes Enforcement Network, "Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System (FIN-2018-A006)," (Oct. 11, 2018).

[56] *See Imposition of Fifth Special Measure Against the Islamic Republic of Iran as a Jurisdiction of Primary Money Laundering Concern*, Financial Crimes Enforcement Network, 84 Fed. Reg. 59,302 (Nov. 4, 2019).

[57] 31 C.F.R. § 1022.210(d)(2).

[58] 31 C.F.R. § 1022.210(d)(3).

operated for almost two years without requiring any AML training to Binance personnel. When Binance eventually began providing training in June 2019, it was only providing that training to select personnel. In fact, the vast majority of Binance personnel employed before July 2020 may not have received any AML training at all, and the early training that Binance provided was insufficient. For example, it included no specificity as to the products and services being offered to Binance customers through its platform. Significantly, the training also failed to cover the risks posed by its "No-KYC" accounts. Personnel were also not given training or tools to mitigate money laundering and terrorist financing risks associated with these accounts (*e.g.*, noting when the same person opens multiple "No-KYC" accounts; identifying structuring to evade Binance's two bitcoin threshold for collecting customer information; or detecting potentially suspicious transactions involving AECs).

9. Binance's Failure to Provide for Independent Review of its AML Program

As an MSB, Binance is required to provide for independent review to monitor and maintain an adequate AML program. The scope and frequency of the review must be commensurate with the risk of financial services provided by the MSB.[59] For most of the Relevant Time Period, Binance failed to conduct adequate independent testing with a scope and frequency commensurate with the risk of financial services. With respect to frequency, Binance did not arrange for any audits of its AML program until March 2020, nearly three years after its initial launch. Given the size of Binance's operations and the nature of the products and services offered by the platform,

[59] 31 C.F.R. § 1022.210(d)(4).

the timing of this report did not meet the requirement that independent testing be conducted with a frequency commensurate with its risk profile.

When a test was finally conducted in March 2020, it fundamentally failed to assess key elements of Binance's operations. The testing only looked at accounts for which there was a fiat-to-CVC nexus—entirely overlooking the money laundering and terrorist financing risks associated with any CVC-to-CVC activity on the platform. The review also focused only on customers that went through the KYC process, entirely excluding "no-KYC" customers. Even then, the review only examined 31 Binance accounts in total (25 individuals and 6 corporate customers, only one of which was rated as high-risk by Binance). This review was facially inadequate based on the sample size alone given the immense size and scale of Binance's operations. It also failed to assess controls applicable to "no KYC" users, a known and immense source of risk for Binance's platform. Significantly, the test included no transaction testing at all. Without transaction testing, an independent test cannot effectively determine if potentially suspicious transactions are handled appropriately, including whether suspicious activity reports were appropriately filed.

The scope of the independent testing also did not include an adequate comprehensive assessment of the geographical risks Binance faced given its global presence. Despite Binance's own 2020 risk assessment listing a risk of "unknowingly expos[ing] Binance to higher risk jurisdictions," and highlighting that Binance supposedly complied FATF and OFAC lists and conducted IP monitoring from the jurisdictions in which Binance purports to not do business, the independent test failed to assess controls around any of these processes. The review also did not assess geofencing controls that limit exposure to most jurisdictions given the paltry sample size. There was no assessment of whether Binance was conducting transactions with customers in

countries designated by FATF on the gray or blacklist. In sum, the review was inadequate and unreliable for assessing Binance's most significant risks.

F. Failure to File Suspicious Activity Reports

The gaps and deficiencies in Binance's approach to AML compliance resulted in a substantial volume of suspicious transactions—in number and overall value—processed through Binance accounts, none of which were reported to FinCEN as required.[60] In fact, Binance filed no SARs with FinCEN throughout the Relevant Time Period. FinCEN identified well over a hundred thousand suspicious transactions that Binance failed to timely and accurately report to FinCEN. Moreover, these failures to report suspicious activity resulted from Binance's initial policy and practice failures that delayed reporting from FinCEN and law enforcement. The former Chief Compliance Officer reported to other Binance personnel that the senior management policy was to never report any suspicious transactions. Binance has taken significant recent steps to enhance its compliance program, including committing substantial resources to address the types of compliance gaps addressed below. As part of its resolution with FinCEN, Binance has committed to a formal SAR lookback.

The unreported suspicious transactions fall into the following categories: ransomware, terrorist financing, high-risk jurisdictions, darknet markets and scams, and child sexual abuse material.

1. *Ransomware*

Ransomware is malicious software that restricts the victim's access to a computer in exchange for a specified ransom, usually paid in bitcoin.[61] If the specified ransom is not paid, the

[60] *See* Section II. C.

[61] FinCEN published advisories in September 2016 and July 2019, respectively, regarding the risk associated with business email compromise, a closely related area of concern to ransomware. *See* Financial Crimes Enforcement

victim may be threatened with the loss or exposure of their personal data, including personally identifiable information (PII), such as account numbers and social security numbers. Some ransomware operators, including those located in Iran and North Korea, have purposefully targeted U.S. hospitals, schools, and other vital public services. Following the 2017 FinCEN enforcement action against BTC-e—citing BTC-e's facilitation of ransomware payments and its failure to report any of these transactions—Binance reportedly became one of the large receivers of ransomware proceeds. Binance was aware of the significant uptick in ransomware activity as early as February 2019.

In fact, Binance was aware of many specific movements of ransomware proceeds through the platform, yet it failed to file SARs with FinCEN. Binance's third-party service provider identified Binance.com deposit addresses as directly linked to ***millions of dollars'*** worth of Nozelesn ransomware[62] proceeds. Binance's compliance team determined these same Binance addresses also had indirect exposure to darknet markets and mixing, which are further indicia of money laundering. Nevertheless, on one occasion in 2019, Binance's former Chief Compliance Officer instructed his team to take no action as the addresses were associated with a high-value client who had indirect exposure to a darknet market. In a separate incident Binance was notified of a ransomware victim by law enforcement, Binance required an indemnity from law enforcement

Network, Advisory to Financial Institutions on E-mail Compromise Fraud Schemes, FIN-2016-A003 (Sept. 6, 2016); Financial Crimes Enforcement Network, *Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes* FIN-2019-A005, (July 16, 2019). On October 1, 2020, FinCEN and OFAC issued advisories to combat ransomware scams and attacks. *See* Financial Crimes Enforcement Network, FIN-2020-A006, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, Financial Crimes Enforcement Network (Oct. 1, 2020); Office of Foreign Assets Control, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, (Oct. 1, 2020).

[62] Nozelesn is a strain of ransomware spread by spam that encrypts the victims' files and requires payment in Bitcoin via TOR that started in July 2018.

prior to providing any reporting. Although Binance took action to protect the victim, no SARs were filed with FinCEN on either incident.

Binance also failed to file SARs on transactions it processed involving the Conti group,[63] after receiving unsolicited reports from their third-party service providers about such attackers using the Binance platform. In May 2022, Binance received a report detailing how Conti was moving illicit proceeds through accounts on its platform. The report included specific CVC wallet addresses and methodologies associated with over $12 million of CVC that traced specifically from Conti attackers to accounts at Binance. Although Binance took internal action to address these allegations, Binance failed to file SARs with FinCEN on these transactions.

Binance addresses transacted directly with CVC obtained via attacks associated with at least 24 different unique strains of ransomware, including: Bitpaymer, Cerber, Cryptolocker, CryptoWall, CrySIS-Dharma, Erebus, Hermes, Locky, NetWalker, NotPetra, Nozelesn, Phobos, Popotic, Ryuk, SamSam, Satan, Snatch, Sodinokibi, Spora, TorrentLocker, and both strains of WannaCry. Gaps in Binance's controls and policies resulted in it being a direct counterparty with ransomware-associated addresses in hundreds of transactions that were each worth $2,000 or more, and in the aggregate worth tens of millions of dollars. Although Binance routinely worked with law enforcement when notified, it failed to file SARs with FinCEN and deprived law enforcement of critical information regarding this illicit activity.

2. *Terrorist Financing*

Binance failed to file SARs with FinCEN on significant sums being transmitted to and from entities officially designated as terrorist organizations by the United States and United

[63] Conti is a "Ransomware-as-a-Service" group that has links to the Russian government and has attacked companies and persons in the United States.

Nations, as well as high-risk exchanges associated with terrorist financing activity. Binance user addresses were found to interact with bitcoin wallets associated with the Islamic State of Iraq and Syria (ISIS), Hamas' Al-Qassam Brigades, Al Qaeda, and the Palestine Islamic Jihad (PIJ). Although no SARs were filed with FinCEN, Binance has proactively cooperated with global law enforcement and blockchain vendors to combat terrorism financing.

Al-Qaeda is a designated foreign terrorist organization founded in 1988 by Osama bin Laden and other Islamic extremists, responsible for civilian and military attacks.[64] FinCEN observed more than 200 direct bitcoin transactions, in the aggregate worth several hundred thousand dollars, with Al-Qaeda-associated CVC wallets, and several of these were for an amount over $2,000 during the Relevant Time Period.

The al-Qassam Brigades is the military wing of the Palestinian Hamas organization. Currently, the al-Qassam Brigades are listed as a terrorist organization by the United States and multiple other countries and organizations.[65] The al-Qassam Brigades' CVC fundraising began in early 2019 with advertisements on Twitter to "Donate to Palestinian Resistance via Bitcoin."[66] FinCEN observed multiple direct bitcoin transactions worth over $2,000 with these CVC wallets during the Relevant Time Period. Binance received reports from its third-party service provider in April 2019 identifying Hamas-associated transactions and filed no SARs with FinCEN. Instead, Binance's former Chief Compliance Officer attempted to influence how its third-party service provider reported on Binance's conduct. Binance has cooperated with Israeli law enforcement in numerous seizures related to the al Qassam Brigades.

---

[64]U.S. Department of State, *Foreign Terrorist Organizations*, (Al-Qaeda designated Oct. 8, 1999).

[65] U.S. Department of State, *Foreign Terrorist Organizations*, (Hamas designated Oct. 8, 1997); U.S. Department of State, *Country Reports on Terrorism 2019* (Apr. 2019).

[66] Department of Justice, *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns*, (Aug. 13, 2020).

ISIS, formerly known as al-Qaeda in Iraq, is responsible for civilian and military attacks and has been designated a foreign-terrorist organization since 2004.[67] FinCEN observed multiple direct transactions between Binance and ISIS-associated CVC wallets during the Relevant Time Period. In one instance, in July 2020, after a third-party service provider flagged accounts associated with ISIS and Hamas, the former Chief Compliance Officer described it as "[e]xtremely dangerous for our company" and instructed compliance personnel to "[c]heck if he is a VIP account, if yes, to… ***[o]ffboard the user but let him take his funds and leave***. ***Tell him that third party compliance tools flagged him***." Binance failed to file a SAR on transactions related to an individual designated by OFAC for support of a terrorist group. The individual was allowed to keep an account for several years in withdrawal-only status after designation and withdraw their balance. Binance's current compliance program would not permit users identified as associated with terrorist financing to remain on the platform or remove funds.

PIJ is a Sunni Islamist militant group seeking to establish an Islamist Palestinian state that is committed to the destruction of Israel and has been designated as a foreign terrorist organization since 1997.[68] FinCEN's investigation identified dozens of former Binance users with tens of millions of dollars in transactions with an identified PIJ network. Binance failed to file a SAR with FinCEN on this activity some of which occurred late in the Relevant Time Period.

Binance also failed to file a SAR with FinCEN on its connections to BuyCash, a money transmitter that OFAC designated in October 2023 for its involvement in Hamas fundraising, as

[67] U.S. Department of State, *Foreign Terrorist Organizations*, (Islamic State of Iraq and the Levant designated Dec. 17, 2004).

[68] U.S. Department of State, *Foreign Terrorist Organizations*, (PIJ designated Oct. 8, 1997); Director of National Intelligence, *Foreign Terrorist Organizations*: *Palestine Islamic Jihad* (Feb. 2023).

well as ties to al-Qa'ida and ISIS.[69] Prior to OFAC's designation of BuyCash, Binance was aware of extensive suspicious activity involving this entity—including connections related to terrorist organizations—but failed to file a SAR with FinCEN.

Similarly, Binance failed to file SARs with FinCEN on transactions involving two Syria-based money transmitters, primarily in 2019 and 2020. Based on public reporting, one of these Syria-based money transmitters operates a 24-hour phone line to assist clients—including Russian speaking foreign fighters—in setting up accounts on Binance. Both money transmitters' ties to terrorist financing have been widely reported for years, including ties to al-Qaeda campaigns that were the subject of a significant DOJ action unsealed in August 2020.[70] In sum, Binance failed to file SARs with FinCEN on these transactions and notified at least one customer involved in suspicious activity. Binance's current compliance program would prohibit the users described above from remaining on the platform or removing funds.

3. *Iranian Counterparties, Including SDNs*

FinCEN identified hundreds of thousands of direct, randomly matched internal trades through Binance's matching engines between U.S. users and Iranian users. As noted above, FinCEN has repeatedly warned about risks associated with transactions conducted with Iran. FinCEN named Iran a jurisdiction of "primary money laundering concern" in a rulemaking finalized in 2019. Of particular concern to FinCEN is that Binance users effected transactions with Iranian CVC exchanges without filing SARs: Binance user wallets effected a significant volume of direct transactions with various Iranian CVC exchanges, each worth more than $2,000

[69] Office of Foreign Assets Control, *Following Terrorist Attack on Israel, Treasury Sanctions Hamas Operatives and Financial Facilitators*, (Oct. 18, 2023).

[70] Department of Justice, *Global Disruption of Three Terror Finance Cyber-Enabled Campaign*, (Aug. 13, 2020).

and in the aggregate worth the equivalent of over half a billion dollars. The Iranian entities involved in these transactions include Iranian VASP 1.[71] No SARs were filed with FinCEN.

The total also includes several transactions with CVC wallets associated with sanctioned entities and individuals, including: (i) EnExchanger, an Iranian entity designated for assisting the cyber actors behind the SamSam ransomware attacks;[72] and (ii) Ahmad Khatibi Aghada, an individual associated with the sanctioned Iranian Revolutionary Guard Corps (IRGC) that engaged in ransomware activities.[73] Binance failed to file SARs with FinCEN on any of these transactions, even after OFAC's designations.

Binance was similarly aware of other Iran-related illicit transactions that occurred on the Binance.com platform but filed no SARs with FinCEN. For example, prior to the institution of full KYC, IranVisaCart, and other illicit actors maintained accounts with Binance, taking advantage of Binance's policies surrounding opening multiple accounts with weak or no KYC. [74] Binance was made aware of these accounts and the related illicit transactions as early as 2019, and filed no SARs with FinCEN.

Binance has substantially enhanced its sanctions and AML compliance program to seek to address the presence of sanctioned and U.S. persons on the platform.

---

[71] Financial Crimes Enforcement Network, *Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System*, FIN-2018-A006, (Oct. 11, 2018). An internal Binance report from January 2020 indicated that Binance was entering into discussions to provide its Binance Cloud product to Iranian VASP 1; the Binance cloud product operates in a manner similar to the Exchange Broker program (*e.g.*, clients of Binance's customers are allowed to access Binance's central order book), except that Binance Cloud included additional services, such as IT hosting.

[72] Office of Foreign Assets Control, *Treasury Designates Iran-based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses*, (Nov. 28, 2018).

[73] Office of Foreign Assets Control, *Treasury Sanctions IRGC-affiliated Cyber Actors for Roles in Ransomware Activity*, (Sept. 14, 2022).

[74] Office of Foreign Assets Control, *Treasury Designates Iran-based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses*, (Nov. 28, 2018).

4. *Darknet Markets and Proceeds of Scams, Frauds, and Other Illicit Activity*

Binance user addresses transacted directly with darknet marketplaces and other illicit markets. Such markets facilitate the purchase and sale of illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband.[75] FinCEN identified CVC moving directly to Binance users from wallets associated with cybercriminals engaged in large-scale hacks, account takeovers, and other criminal organizations and activities.

Prior to its designation, Binance received a substantial number of transactions directly from the world's largest darknet market, Hydra Market, which was sanctioned by OFAC in April 2022.[76] Hydra Market is a Russia-based, TOR-network operated darknet marketplace in operation since at least 2014 that sells illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. Binance users completed over fifteen thousand direct transactions with Hydra Market addresses, each worth more than $2,000, and in the aggregate worth more than $250 million. At least 25 Binance customers received over $1 million each directly from Hydra. One customer received over $6 million from Hydra Market. Binance personnel went so far as to instruct their high value clients on how to continue processing transactions through the platform in July 2020: "***Can let him know to be careful with his flow of funds, especially from darknet like hydra[.] He can come back with a new account[,] [b]ut this***

[75] , Financial Crimes Enforcement Network, *Advisory on Illicit Activity Involving Convertible Virtual Currency,* FIN-2019-A003, (May 9, 2019).

[76] Office of Foreign Assets Control, *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex*, (Apr.5, 2022).

current one has to go, it[']s tainted." Binance failed to file a SAR with FinCEN on this, or any activity, associated with Hydra Market even after its designation by OFAC and seizure.[77]

Binance also received substantial proceeds from the September 2018 hack of the Zaif exchange by facilitating hundreds of transactions involving stolen funds. Binance acknowledged that CVC wallet addresses on Binance were used to launder 1,451.7 bitcoin (over $9.5 million) from the hack, which was broken into 1.99-2 (over $13,000) bitcoin transactions. These amounts indicate that the hackers were taking advantage of Binance's prior 2 bitcoin no-KYC policy and effected transactions to evade this threshold. A senior Binance manager recommended against closing these accounts, stating, "I think there is no meaning to take more effort to these addresses. It's a type of standard money laundering," but offered to provide documentation to law enforcement if asked. In sum, Binance filed no SARs with FinCEN despite its own observation of money laundering taking place. Binance works closely with law enforcement agencies world-wide related to this type of illicit activity, including Hydra, darknet markets, and hacks.

5. *Child Sexual Abuse Material*

FinCEN observed over a thousand direct bitcoin and ether transactions, worth hundreds of thousands of dollars, with child exploitation-associated CVC wallet addresses, including at least three separate marketplaces dealing in child sexual abuse materials (CSAM). Multiple CVC wallet addresses associated with Binance received thousands of dollars directly from the CSAM website Dark Scandals. Dark Scandals was a site hosted on both the Darknet and Clearnet that featured videos and depictions of child pornography. [78] On March 12, 2020, the Department of Justice

[77]Department of Justice, *Justice Department Investigation Leads To Shutdown Of Largest Online Darknet Marketplace*, (Apr. 5, 2022).

[78]Department of Justice, *Dutch National Charged in Takedown of Obscene Website Selling Over 2,000 "Real Rape" and Child Pornography Videos, Funded by Cryptocurrency*, (Mar. 12, 2020).

indicted a Dark Scandals administrator for various counts of Distribution of Child Pornography, Production and Transportation of Obscene Matters for Sale or Distribution, and Engaging in the Business of Selling or Transferring Obscene Matter.[79] Although Binance took internal action to address Dark Scandals, even after the indictment was made public, Binance never filed SARs with FinCEN on any transactions involving Dark Scandals. Binance combats identified exposures to CSAM-related entities and has worked proactively with law enforcement to combat CSAM.

[79] Department of Justice, *Dutch National Charged in Takedown of Obscene Website Selling Over 2,000 "Real Rape" and Child Pornography Videos, Funded by Cryptocurrency*, (Mar. 12, 2020).

III. VIOLATIONS

FinCEN has determined that Binance willfully violated the BSA and its implementing regulations during the Relevant Time Period with regard to its obligation to register as an MSB, maintain an effective AML program, and report suspicious transactions. Specifically, FinCEN has determined that, as of January 10, 2018,[80] Binance was required to register as an MSB with FinCEN and willfully failed to do so in violation of 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380. FinCEN has also determined that, as of October 12, 2017,[81] Binance was required to develop, implement, and maintain an effective AML program that was reasonably designed to prevent it from being used to facilitate money laundering and the financing of terrorist activities, and willfully failed to do so in violation of 31 U.S.C. § 5318(h)(1) and 31 C.F.R. § 1022.210. Additionally, FinCEN has determined that, throughout the Relevant Time Period, Binance was required to accurately, and timely, report suspicious transactions to FinCEN, and willfully failed to do so in violation of 31 U.S.C. § 5318(g) and 31 C.F.R. § 1022.320.

As explained in detail above: (1) Binance personnel knew that the company was doing extensive business in the United States and devised a strategy to retain the commercial benefits associated with this business without registering with FinCEN as an MSB; (2) Binance delayed implementation of an AML Program and maintained categorical gaps (most notably with respect to exempting large numbers of users from KYC requirements, allowing Exchange Brokers free reign, and failing to implement risk-based controls applicable to AECs) once implemented; and (3) Binance failed to file any SARs with FinCEN despite processing billions of dollars' worth of transactions involving a broad range of illicit activity, including ransomware actors and sanctioned entities.

[80] See note 6, *supra*.

[81] See note 6, *supra*.

IV. ENFORCEMENT FACTORS

FinCEN has considered all of the factors outlined in the Statement on Enforcement of the Bank Secrecy Act issued August 18, 2020, when deciding whether to impose a Civil Money Penalty in this matter.[82] The following factors were particularly relevant to FinCEN's evaluation of the appropriate disposition of this matter, including the decision to impose a Civil Money Penalty and the size of that Civil Money Penalty.

- **Nature and seriousness of the violations, including the extent of possible harm to the public**:

  Binance's violations were not only substantial in both number and USD-equivalent value, but they also exposed the public to significant possible harm. Binance's willful failure to register as an MSB persisted over an extended period, during which time Binance senior management misled U.S. authorities. Binance operated for over a year with no AML program, and the AML program that it subsequently implemented was ineffective and contained categorical gaps. Binance personnel had actual knowledge that illicit activity was flowing through the platform as the result of deficient KYC procedures, yet several years elapsed before Binance took any steps to begin remediating these gaps. Binance's willful failure to implement an effective AML program directly led to the platform being used to process transactions related to child exploitation material, ransomware attacks, darknet and other illicit marketplaces, unregistered convertible virtual currency mixing services used to launder illicit proceeds, high-risk jurisdictions, individuals listed on OFAC's SDN List, terrorist financing, and stolen funds or

[82] FinCEN, Statement on Enforcement of the Bank Secrecy Act (Aug. 18, 2020), https://www.fincen.gov/sites/default/files/shared/FinCEN%20Enforcement%20Statement_FINAL%20508.pdf.

other illicit proceeds. Binance's willful failure to report to FinCEN hundreds of thousands of suspicious transactions inhibited law enforcement's ability to disrupt the illicit actors.

- **Impact or harm of the violations on FinCEN's mission to safeguard the financial system from illicit use, combat money laundering, and promote national security**:

  Binance's violations extensively harmed FinCEN's mission to safeguard our financial system from illicit use. Despite doing business wholly or in substantial part within the U.S., Binance willfully failed to register with FinCEN while obfuscating its continuing relationships with commercially important U.S. trading firms. The ineffective AML program that Binance eventually implemented contained categorical gaps. These gaps allowed illicit actors to effect suspicious transactions through Binance, which Binance willfully failed reported to FinCEN. As the world's largest CVC exchange, Binance's scale has had a significant effect on our financial system by exposing the U.S. financial system to a significant volume of illicit financial activity. FinCEN identified hundreds of thousands of potentially suspicious transactions that went through the Binance platform during the Relevant Time Period, yet Binance failed to file a single SAR with FinCEN.

- **Pervasiveness of wrongdoing within an entity, including management's complicity in, condoning or enabling of, or knowledge of the conduct underlying the violations:**

  Binance senior management not only allowed violations to persist for a prolonged period, but was also complicit in the misconduct. Binance's senior management was aware of its obligation to register as an MSB, but instead of complying with this obligation, directed Binance personnel to obscure the nature and extent of its ties to the United States. Similarly, Binance senior management was aware of the ineffective nature of its AML program and that illicit actors were exploiting Binance's AML weaknesses to effect suspicious transactions. Instead of addressing these AML deficiencies, senior management instructed Binance

personnel to not file SARs and to obstruct law enforcement investigations. Binance was also not forthcoming about the ongoing nature of its registration-related violations that continued on the platform even well after FinCEN initiated its investigation.

- **History of similar violations, or misconduct in general, including prior criminal, civil, and regulatory enforcement actions:**

  The violations described herein have persisted since Binance began operations. Multiple U.S. authorities have filed lawsuits against Binance for other violations of U.S. law.

- **Financial gain or other benefit resulting from, or attributable to, the violations:**

  Binance prioritized rapid growth and expansion without commensurate and timely investment in compliance with its regulatory obligations. Binance's policy of dispensing with all KYC requirements for accounts that withdrew less than two bitcoin per day exemplifies this failure. This policy allowed Binance to attract customers rapidly and thereby achieve the network effects and economies of scale necessary to become the largest CVC platform. This policy exposed the platform to extensive risk of abuse by illicit actors. Binance also prioritized attracting and maintaining relationships with large U.S. market makers to drive activity on the platform and increase profits, while flagrantly evading regulatory obligations for U.S. MSBs, and misleading regulators, for more than four years. As a result of these actions, Binance now conducts roughly five times the daily trading volume of its next largest competitor. Similarly, Binance has padded its bottom line by delaying investments in regulatory compliance tools and personnel. Binance has continued to announce its expansion and additional new products, services, sponsorships, and partnerships before it has addressed existing compliance issues. All of these decisions gave the company an unfair competitive advantage in the marketplace as compared to other companies offering similar products and services that were investing in appropriate technology and personnel to comply with the BSA.

- **Presence or absence of prompt, effective action to terminate the violations upon discovery, including self-initiated remedial measures:**

  During the Relevant Time Period, Binance remained out of compliance with the BSA. Although Binance has made certain investments in AML compliance and some changes to its policies and practices, these actions should be afforded less weight because: (i) the most significant changes occurred only after Binance became the subject of investigations by FinCEN and other authorities, and some of these changes were implemented only recently in connection with negotiations to resolve FinCEN's investigation; (ii) Binance created a U.S. entity, Binance.us, but delayed offboarding its most lucrative U.S. clients; and (iii) although Binance has voluntarily (but selectively) cooperated with certain requests from U.S. law enforcement, it has not filed a single SAR with FinCEN. As part of discussions with FinCEN to resolve its investigation, Binance agreed to cease its practice of opening anonymous subaccounts and permitting them to transact on or through Binance.com and begin undertaking remedial measures to appropriately mitigate the risks posed by AECs. Binance has also agreed to retrospectively review its customers' historical transactions to identify suspicious activity that it failed to report. These recent remedial steps are significant, but far from prompt. Recently, Binance has demonstrated an improved commitment to AML compliance.

- **Timely and voluntary disclosure of the violations to FinCEN:**

  FinCEN's investigation was proactive and was not the result of an examination or disclosures made by law enforcement or by Binance itself.

- **Quality and extent of cooperation with FinCEN and other relevant agencies, including as to potential wrongdoing by its directors, officers, employees, agents, and counterparties:**

  Although Binance provided dozens of productions, these productions frequently were delayed, did not satisfy FinCEN's enumerated requests and/or were incomplete. Significantly, Binance

refused to fully respond to FinCEN's basic questions about continuing U.S. customer activity on its platform. Binance's incomplete responses and patently unreasonable delays in providing readily available information reflect its disdain for regulatory obligations. Binance's recalcitrant approach to FinCEN's investigation is consistent with earlier efforts by Binance senior management to mislead U.S. authorities. More recently, the quality and extent of Binance's cooperation has improved, including changing certain practices that had been the subject of significant FinCEN concerns.

- **Systemic Nature of the Violations. Considerations include, but are not limited to, the number and extent of violations, failure rates (*e.g.*, the number of violations out of total number of transactions), and duration of violations:**

  As explained above, the violations that FinCEN identified were numerous, substantial in aggregate value and occurred over an extended period.

- **Whether another agency took enforcement action for related activity. FinCEN will consider the amount of any fine, penalty, forfeiture, and/or remedial action ordered:**

  Following separate but parallel investigations led by the CFTC, Department of Justice, and OFAC, Binance has agreed to pay approximately $4.316 billion to resolve these investigations. This amount includes the below civil money penalty imposed by FinCEN.

V. CIVIL PENALTY

A. Legal Background

FinCEN may impose a Civil Money Penalty of $9,966 per day for willful violations of the requirement to register as an MSB.[83]

[83] *See* 31 U.S.C. § 5330(e) and 31 C.F.R. § 1010.821.

FinCEN may impose a Civil Money Penalty of $67,544 per day for willful violations of the requirement to implement and maintain an effective AML program.[84]

For each willful violation of a SAR reporting requirement, FinCEN may impose a Civil Money Penalty not to exceed the greater of the amount involved in the transaction (capped at $270,180 or $67,544).[85]

B. Civil Penalty Determination

After considering all the facts and circumstances in this case, as well as the enforcement factors discussed above, FinCEN has determined to impose a Civil Money Penalty of $3.4 billion in this matter. FinCEN has agreed to credit against the $3.4 billion Civil Money Penalty payments of $2.47 billion to the Department of Justice and the CFTC. In addition, FinCEN has agreed to suspend $150 million of the Civil Money Penalty pending Binance's compliance with the Undertakings set forth below. Accordingly, Binance shall make a payment for the Civil Money Penalty of $780 million to the U.S. Department of the Treasury pursuant to the payment instructions that will be transmitted to Binance upon execution of this Consent Order.

VI. UNDERTAKINGS

By execution of this Consent Order, Binance agrees to the following Undertakings. If Binance fails to comply with any of the requirements of these Undertakings, which shall be determined by FinCEN in its sole discretion, the $150,000,000 suspended penalty will be triggered, and Binance will be required to pay the suspended penalty. This payment must be paid in full within

[84] 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.821.

[85] 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.821.

10 days of receipt of written notice by FinCEN that the suspended penalty is triggered and payment is required.

A. Independent Compliance Monitor

1. Promptly after FinCEN's selection pursuant to Paragraph 3 below, Binance agrees to retain an independent compliance monitor (Monitor). The Monitor's duties and authority, and the obligations of Binance with respect to FinCEN, as well as OFAC, the CFTC, and the Department of Justice, as applicable, are set forth in Attachment A, which is incorporated by reference into this Consent Order. Binance is responsible for ensuring that the Monitor carries the responsibilities set forth in Attachment A. Within 30 days after the Effective Date of this Consent Order, Binance shall submit a written proposal identifying no less than three candidates to act as Monitor, and, at a minimum, providing the following:

a. a description of each candidate's qualifications and credentials in support of the evaluative considerations and factors listed below;

b. a written certification by Binance that it will not employ, contract with, or otherwise have any affiliation with the Monitor, any member of the Monitor's team or the Monitor's firm for a period of not less than two years from the date of the termination of the Term of the Monitorship (as defined below);

c. a written certification by each of the candidates that they are not a current or recent (*i.e.*, within the prior two years) employee, officer, director, agent, or representative of Binance and hold no interest in, and have no relationship with, Binance, its subsidiaries, or affiliates, or their respective employees, officers, directors, agents, or representatives;

d. a written certification by each of the candidates that they have notified provided notice of their candidacy to any clients that the candidate represents in a matter involving

FinCEN, and that the candidate has either obtained a waiver from those clients or has withdrawn as counsel in the other matter(s); and

e. a statement identifying the candidate that is Binance's first, second, and third choice to serve as the Monitor.

2. The candidates to act as Monitor or their team members shall have, at a minimum, the following qualifications (Minimum Qualifications):

a. demonstrated expertise with respect to the BSA, and sanctions regulations administered by OFAC;

b. experience designing and/or reviewing corporate compliance policies, procedures, and internal controls, including AML controls such as transaction monitoring, conducting CVC blockchain analysis to determine compliance with the requirements of the BSA, integration of AML in product governance, and sanctions compliance policies, procedures, and internal controls;

c. the ability to access and deploy resources, including the work of outside consultants, to discharge the Monitor's duties as described in this Consent Order; and

d. sufficient independence from Binance to ensure effective and impartial performance of the Monitor's duties as described in this Consent Order.

3. FinCEN retains the right, in its exclusive discretion, to choose the Monitor from among the candidates proposed by Binance, though Binance may express its preference(s) among the candidates. Monitor selections shall be made in keeping with FinCEN's commitment to diversity and inclusion. If FinCEN determines, in its exclusive discretion, that any candidate is not, in fact, qualified to serve as the Monitor, or if FinCEN, in its exclusive discretion, is not satisfied with any candidate proposed, FinCEN reserves the right to reject that candidate. In the

event that FinCEN rejects any proposed candidate, Binance shall propose additional candidates within 30 business days after receiving notice of the rejection so that three qualified candidates are proposed. This process shall continue until a Monitor acceptable to both parties is chosen, unless FinCEN, at any time and in its sole discretion, determines that Binance is not recommending candidates in good faith. If FinCEN makes such a determination, FinCEN may solicit applications from the public and select a Monitor from among those applicants meeting the Minimum Qualifications. FinCEN will use its best efforts to complete the selection process within 60 days of the execution of this Consent Order. If the Monitor resigns or is otherwise unable to fulfill their obligations as set out herein and in Attachment A, Binance shall within 20 days recommend a pool of three qualified candidates from which FinCEN will choose a replacement through the process set out herein.

4. The Monitor's term shall be five years from the date on which the Monitor is retained by Binance (Term of the Monitorship). The Monitor shall be retained at Binance's own expense throughout the Term of the Monitorship. In the event that FinCEN finds, in its exclusive discretion, in consultation with OFAC, the CFTC, or the Department of Justice, as appropriate, that there exists a change in circumstances sufficient to eliminate the need for the Monitor, and that the other provisions of this Consent Order have been satisfied, the Term of the Monitorship may be terminated early. Without prejudice to FinCEN's right to proceed in the event of a Breach of this Consent Order, FinCEN may, in consultation with the Monitor, extend the Term for up to a total additional time of one year.

5. The Monitor's powers, duties, and responsibilities, as well as additional circumstances that may support an extension of the Monitor's term or its early termination, are set forth in Attachment A. Binance agrees that it will not employ, contract with, or otherwise be

affiliated with the Monitor or the Monitor's firm for a period of not less than two years from the date on which the Monitor's term expires. Nor will Binance discuss with the Monitor, any member of the Monitor's team or the Monitor's firm the possibility of further employment or affiliation at any time during the Term of the Monitorship, and for a period of two years after the Monitor's term.

6. Binance agrees to require that its wholly-owned subsidiaries and affiliates comply with the requirements and obligations set forth in Attachment A, provided that compliance with such requirements and obligations would not violate locally applicable laws and regulations or the instructions of local regulatory agencies.

B. Offboarding of U.S. Users

7. Within 90 days from the retention of the Monitor, Binance, in consultation with the Monitor, will complete a review of: (i) Binance.com users with ties to the United States (U.S. users) identified by FinCEN in accordance with pre-resolution negotiations with Binance; and (ii) all of the top 35 Binance.com users by revenue. The review will identify U.S. users for offboarding by applying the policies, procedures, and internal controls revised pursuant to Binance's negotiations with FinCEN, and, as applicable, the CFTC, and Department of Justice, as well as any of the Monitor's recommended enhancements to such. policies, procedures, and internal controls.

8. Within 21 days from the completion of this review, Binance will deliver to the Monitor and FinCEN a report summarizing the findings of its review and identifying the U.S. users that Binance has offboarded or restricted, or will, within the time required by Paragraph 9, offboard or restrict. Binance will comply with requests for additional information about the review of U.S.

users as well as with findings and recommendations from the Monitor or FinCEN that Binance modify or update its report, and offboard or restrict additional users in connection with this review.

9. No later than 60 days after providing the report summarizing findings of its review to the Monitor and FinCEN, Binance will: (i) finalize the offboarding or restriction of all identified U.S. users; and (ii) provide a certification to FinCEN signed by Binance's Chief Compliance Officer attesting to the completion of such offboarding or restriction.

10. For the duration of the Term of the Monitorship, Binance shall undertake an annual review to confirm the absence of U.S. users on Binance.com based on a review of: (i) any Binance.com users with ties to the U.S. identified by FinCEN; and (ii) all of the top 35 Binance.com users by revenue for the prior calendar year. Binance shall provide reports of such annual reviews to the Monitor and FinCEN no later than January 1st of each calendar year during the Term of the Monitorship. Within 30 days of providing each annual report summarizing findings of its review to the Monitor and FinCEN, Binance will: (i) finalize the offboarding or restriction of all identified U.S. users; and (ii) provide a certification to FinCEN signed by Binance's Chief Compliance Officer attesting to the completion of such process.

C. SAR Lookback

11. Within 60 days from the retention of the Monitor, the Monitor will propose a qualified independent consultant (SAR Lookback Consultant) for Binance to hire, at its own expense, to conduct a SAR Lookback Review.[86] The Monitor has the right to veto the engagement of a SAR Lookback Consultant that the Monitor deems unsuitable to complete the SAR Lookback Review. The SAR Lookback Consultant will review transactions or attempted transactions by, at, or through Binance, that occurred from January 1, 2018 through December 31, 2022 (Covered

[86] Subject to FinCEN approval, the Monitor may elect to serve as the SAR Lookback Consultant.

Transactions) to determine whether activity was properly identified and reported under 31 U.S.C. § 5318(g) and implementing regulations.

12. Within 90 days from the date of engagement of the SAR Lookback Consultant, the Monitor will deliver to FinCEN a report summarizing the proposed scope and methodology of the review of the Covered Transactions that the SAR Lookback Consultant plans to conduct (SAR Lookback Scope Report). FinCEN, in consultation with the Monitor, may amend the scope of the review of Covered Transactions within 30 days of FinCEN's receipt of the report summarizing the proposed scope and methodology. Following submission of the SAR Lookback Scope Report to FinCEN, the Monitor will deliver quarterly progress reports to FinCEN documenting the status of the SAR Lookback Review.

13. Within one year from the date of the SAR Lookback Scope Report, and no later than May 2025, the SAR Lookback Consultant will deliver a detailed report (SAR Lookback Report) to FinCEN and Binance that summarizes the methodology and findings of its review and identifies the Covered Transactions that may require a SAR to be filed pursuant to 31 U.S.C. § 5318(g) and its implementing regulations. Binance will make, and will cause the SAR Lookback Consultant to make, interim reports, drafts, work papers, or other supporting materials related to the SAR Lookback Review available to FinCEN upon request. Binance will comply with the findings of the SAR Lookback Consultant, the Monitor, or FinCEN that Binance file SARs on any of the Covered Transactions, and, in the event that any of the SAR Lookback Consultant, the Monitor, or FinCEN recommend that Binance file a SAR on a Covered Transactions, Binance will comply with that recommendation. Subject to approval of FinCEN, Binance may, during the pendency of the SAR Lookback Review, begin to file SARs regarding the Covered Transactions that would have required a report pursuant to 31 U.S.C. § 5318(g) and implementing regulations.

14. No later than 90 days from the date of the SAR Lookback Report, Binance will complete the filing with FinCEN of SARs regarding all of the Covered Transactions identified by the independent consultant as ones that would have required a report pursuant to 31 U.S.C. § 5318(g) and implementing regulations. Binance shall be entitled to one 60-day extension of this SAR filing deadline as of right. Any additional extensions require the written consent of FinCEN in its sole discretion.

D. AML Program Review, Including KYC of Sub-accounts

15. Within 60 days from the date of retention of the Monitor, the Monitor, will propose a qualified independent consultant (AML Program Consultant) for Binance to hire, at its own expense, to conduct a review of the effectiveness of Binance's AML program though an AML Program Review.[87] The Monitor has the right to veto the engagement of an AML Program Consultant that the Monitor deems unsuitable to complete the AML Program Review. The AML Program Review will determine whether Binance complies with the Relevant BSA Provisions . The "Relevant BSA Provisions" for purposes of this Consent Order are Code of Federal Regulations Title 31, Chapter X, Part 1022, except as agreed to between the parties.

16. Within 90 days from the date of Binance's retention of the AML Program Consultant, the AML Program Consultant will provide FinCEN with a report summarizing the proposed scope and methodology of the review of Binance's AML program (AML Program Scope Report). The AML Program Scope Report must include proposed analyses to cover at least the following aspects of Binance's AML Program:

i. High-level Commitment to Compliance: the extent to which Binance's senior management, and, if applicable, directors, provide sufficiently strong, explicit, and

[87] Subject to FinCEN approval, the Monitor may elect to serve as the AML Program Consultant.

visible support and commitment to Binance's AML program, including the rigor of adherence demonstrated through example, as well as reinforcement by all levels of management within Binance to create and foster a culture of ethics and compliance throughout the organization.

ii. Periodic Risk Assessments: the extent to which Binance's AML program includes regular, periodic assessments of Binance's money laundering, terrorist financing, and other illicit financial activity risks based on Binance's business activities, including products, services, distribution channels, customers, intermediaries, and geographic locations.

iii. Policies, Procedures and Internal Controls: the extent to which Binance maintains and enforces clearly articulated and visible corporate AML policies that, with the exception of certain limited reporting obligations, are consistent with the Relevant BSA Provisions and applicable to all officers and employees, and, where necessary and appropriate, Binance's agents; such policies and related procedures and internal controls shall address, at a minimum:

a. verifying customer identification and KYC, including with respect to Binance's controls applicable to Enterprise Users with subaccounts (which shall include confirmation that Binance has completed sufficient KYC for all users with the ability to deposit funds onto or withdraw funds from the platform, and users with to access Binance's central order book), the application of identification and screening requirements to individuals associated with Enterprise Users, the consistent application of proof of

address requirements, and the use of customer identification and KYC data to identify users resident in high risk jurisdictions;

b. the controls associated with Binance's announced exit from Russia, a source of heightened illicit finance risk, initiated through Binance's September 2023 transaction to sell its Russian business to CommEx, including Binance's controls to identify users with a Russian nexus, to prevent access by CommEx to Binance services (including, but not limited to, its central order book), to prevent the re-onboarding to Binance of users offboarded due to their high-risk Russian nexus, to identify and restrict support by Binance of CommEx beyond that required to effect the announced transaction, and to mitigate the residual exposure that Binance will have to Russian illicit finance even after successful completion of the transaction;

c. transaction monitoring, including deposits, withdrawals, on-platform activity, including, in the context of users with subaccounts, the extent to which such controls are effective in identifying specific subaccounts associated with potentially suspicious transactions;

d. identifying suspicious activity and filing reports of such activity in applicable jurisdictions, as appropriate;

e. restricting or offboarding of customers—including the extent to which personnel from Binance's CEO office, VIP team, or other business groups are able to intervene in, or override, related decisions made by compliance personnel;

f. mitigating AML risks associated with privacy enhancing products and services, including the framework that Binance uses to assess which AECs are eligible for listing on Binance.com and the sufficiency of controls that Binance applies to AECs deemed eligible for listing, such as Binance's mitigation of potential evasion or structuring by customers to evade prohibitions on specific privacy enhancing features, the tailoring of transaction monitoring thresholds associated with AECs, and the consideration of AECs in developing and updating customer risk profiles;

g. responding to requests for information from law enforcement, regulators, and supervisors; and

h. creating and retaining other records and filing other reports, as appropriate.

iv. Independence, Resourcing, and Empowerment of Compliance: whether Binance has assigned responsibility to an individual for assurance of its day-to-day AML Program, and the extent of autonomy that individual has from management—including as demonstrated by Binance's governance structures, the ability of compliance personnel to access relevant systems, and the integrity of such systems and associated outputs—as well as the sufficiency of resources and authority to maintain such autonomy.

v. Guidance and Training: the extent to which Binance maintains mechanisms to provide periodic training for all Binance personnel—including training tailored to account for the recipients' roles and responsibilities within Binance, as well as training that incorporates, as permissible under applicable law, Binance's prior compliance failures—and records of successful completion of such training.

vi. Internal Reporting and Related Investigations: the extent to which Binance maintains an effective system for internal, and, where possible, confidential reporting by, as well as protection of, employees, officers, and where appropriate, agents, concerning violations of AML laws, including through the implementation of mechanisms designed to ensure that the system for such reporting is effectively communicated to all potential reporters and that Binance maintains an effective and reliable process with sufficient resources to respond to, investigate, and document the investigation of any such reports.

vii. Enforcement, Discipline, and Employee Compensation: the extent to which Binance maintains mechanisms designed to effectively enforce its AML Program, including to discipline violations and incentivize compliance by implementing policies, procedures, and internal controls to take reasonable steps to remedy harm stemming from misconduct (which may include updates to the AML Program's policies, procedures, and internal controls) and implementing evaluation criteria in its personnel review process to account for actions taken by personnel to ensure compliance with the AML Program.

viii. Independent Testing: whether Binance conducts periodic reviews and tests of its AML program designed to evaluate and improve its effectiveness in preventing and detecting money laundering, terrorist financing and other illicit finance activity, including by taking into account examinations by regulators and auditors, as well as relevant developments and emerging risks in the CVC markets.

17. FinCEN, in consultation with the Monitor, may amend the scope of the review of Binance's AML program through a notification to the Monitor within 30 days of FinCEN's receipt

of the report summarizing the proposed scope and methodology. Following submission of the AML Program Scope Report to FinCEN, the Monitor will deliver quarterly progress reports to FinCEN documenting the status of the AML Program Review.

18. Within 60 days from the end of its review, but no later than one year from the date of its engagement, the AML Program Consultant will submit to FinCEN a written report: (i) addressing the adequacy of Binance's AML program, including, but not limited to, the areas set forth in the AML Program Scope Report; (ii) describing the review performed; and (iii) describing any recommended modifications or enhancements to Binance's AML program. Binance will make, and will cause the AML Program Consultant to make, interim reports, drafts, workpapers or other supporting materials related to the AML Program Review available to FinCEN upon request.

19. Binance, in consultation with the Monitor, will develop a plan to implement any recommendations made in connection with the AML Program Review (Implementation Plan) or, within 90 days after issuance of a report, propose alternatives. The AML Program Consultant will provide a written response to any proposed alternatives within 60 days. Within 180 days after finalization of the Implementation Plan, Binance will provide FinCEN and the Monitor with a written report detailing the extent to which it has adopted and implemented the Implementation Plan. As set forth in Attachment A, Binance's implementation of the recommendations shall be subject to the Monitor's validation reviews.

VII. CONSENT AND ADMISSIONS

To resolve this matter and only for that purpose, Binance admits to the Statement of Facts and Violations set forth in this Consent Order to the extent described above and admits that it willfully violated the BSA and its implementing regulations. Binance consents to the use of the Statement of

Facts, and any other findings, determinations, and conclusions of law set forth in this Consent Order in any other proceeding brought by or on behalf of FinCEN, or to which FinCEN is a party or claimant, and agrees they shall be taken as true and correct and be given preclusive effect without any further proof. Binance understands and agrees that in any administrative or judicial proceeding brought by or on behalf of FinCEN against it, including any proceeding to enforce the Civil Money Penalty imposed by this Consent Order or for any equitable remedies under the BSA, Binance shall be precluded from disputing any fact or contesting any determinations set forth in this Consent Order.

To resolve this matter, Binance agrees to and consents to the issuance of this Consent Order and all terms herein and agrees to make a payment of $780 million pursuant to the payment instructions that will be transmitted to Binance upon execution of this Consent Order. If timely payment is not made, Binance agrees that interest, penalties, and administrative costs will accrue.[88]

Binance understands and agrees that it must treat the Civil Money Penalty paid under this Consent Order as a penalty paid to the government and may not claim, assert, or apply for a tax deduction, tax credit, or any other tax benefit for any payments made to satisfy the Civil Money Penalty. Binance understands and agrees that any acceptance by or on behalf of FinCEN of any partial payment of the Civil Money Penalty obligation will not be deemed a waiver of Binance's obligation to make further payments pursuant to this Consent Order, or a waiver of FinCEN's right to seek to compel payment of any amount assessed under the terms of this Consent Order, including any applicable interest, penalties, or other administrative costs.

Binance affirms that it agrees to and approves this Consent Order and all terms herein freely and voluntarily and that no offers, promises, or inducements of any nature whatsoever have been

[88] 31 U.S.C. § 3717; 31 C.F.R. § 901.9.

made by FinCEN or any employee, agent, or representative of FinCEN to induce Binance to agree to or approve this Consent Order, except as specified in this Consent Order.

Binance understands and agrees that this Consent Order implements and embodies the entire agreement between Binance and FinCEN, and its terms relate only to this enforcement matter and any related proceeding and the facts and determinations contained herein. Binance further understands and agrees that there are no express or implied promises, representations, or agreements between Binance and FinCEN other than those expressly set forth or referred to in this Consent Order and that nothing in this Consent Order is binding on any other law enforcement or regulatory agency or any other governmental authority, whether foreign, Federal, State, or local.

Binance understands and agrees that nothing in this Consent Order may be construed as allowing Binance, its subsidiaries, affiliates, Board, officers, employees, or agents to violate any law, rule, or regulation.

Binance consents to the continued jurisdiction of the courts of the United States over it and waives any defense based on lack of personal jurisdiction or improper venue in any action to enforce the terms and conditions of this Consent Order or for any other purpose relevant to this enforcement action. Solely in connection with an action filed by or on behalf of FinCEN to enforce this Consent Order or for any other purpose relevant to this action, Binance authorizes and agrees to accept all service of process and filings through the Notification procedures below and to waive formal service of process.

VIII. COOPERATION

Binance shall fully cooperate with FinCEN in any and all matters within the scope of or related to the Statement of Facts, including any investigation of its current or former directors, officers, employees, agents, consultants, or any other party. Binance understands that its cooperation pursuant

to this paragraph shall include, but is not limited to, truthfully disclosing all factual information with respect to its activities, and those of its present and former directors, officers, employees, agents, and consultants. This obligation includes providing to FinCEN, upon request, any document, record or other tangible evidence about which FinCEN may inquire of Binance. Binance's cooperation pursuant to this paragraph is subject to applicable laws and regulations, as well as valid and properly documented claims of attorney-client privilege or the attorney work product doctrine.

IX. RELEASE

Execution of this Consent Order and compliance with all of the terms of this Consent Order, settles all claims that FinCEN may have against Binance for the conduct described in this Consent Order during the Relevant Time Period. Execution of this Consent Order, and compliance with the terms of this Consent Order, does not release any claim that FinCEN may have for conduct Binance other than the conduct described in this Consent Order during the Relevant Time Period, or any claim that FinCEN may have against any current or former director, officer, owner, or employee of Binance or any other individual or entity other than those named in this Consent Order. In addition, this Consent Order does not release any claim or provide any other protection in any investigation, enforcement action, penalty assessment, or injunction relating to any conduct that occurs after the Relevant Time Period as described in this Consent Order.

X. WAIVERS

Nothing in this Consent Order shall preclude any proceedings brought by, or on behalf of, FinCEN to enforce the terms of this Consent Order, nor shall it constitute a waiver of any right, power, or authority of any other representative of the United States or agencies thereof, including but not limited to the Department of Justice.

In consenting to and approving this Consent Order, Binance stipulates to the terms of this Consent Order and waives:

A. Any and all defenses to this Consent Order, the Civil Money Penalty imposed by this Consent Order, and any action taken by or on behalf of FinCEN that can be waived, including any statute of limitations or other defense based on the passage of time;

B. Any and all claims that FinCEN lacks jurisdiction over all matters set forth in this Consent Order, lacks the authority to issue this Consent Order or to impose the Civil Money Penalty, or lacks authority for any other action or proceeding related to the matters set forth in this Consent Order;

C. Any and all claims that this Consent Order, any term of this Consent Order, the Civil Money Penalty, or compliance with this Consent Order, or the Civil Money Penalty, is in any way unlawful or violates the Constitution of the United States of America or any provision thereof;

D. Any and all rights to judicial review, appeal or reconsideration, or to seek in any way to contest the validity of this Consent Order, any term of this Consent Order, or the Civil Money Penalty arising from this Consent Order;

E. Any and all claims that this Consent Order does not have full force and effect, or cannot be enforced in any proceeding, due to changed circumstances, including any change in law;

F. Any and all claims for fees, costs, or expenses related in any way to this enforcement matter, Consent Order, or any related administative action, whether arising under common law or under the terms of any statute, including, but not limited to, under the Equal Access to Justice Act. Binance agrees to bear its own costs and attorneys' fees.

XI. VIOLATIONS OF THIS CONSENT ORDER

Determination of whether Binance has failed to comply with this Consent Order, or any portion thereof (including, but not limited to, compliance with the MSB registration requirement and completion of the SAR Lookback Review and the AML Program Review), and whether to pursue any further action or relief against Binance shall be in FinCEN's sole discretion. If FinCEN determines, in its sole discretion, that a failure to comply with this Consent Order, or any portion thereof, has occurred, or that Binance has made any misrepresentations to FinCEN or any other government agency related to the underlying enforcement matter, FinCEN may void any and all releases or waivers contained in this Consent Order; reinstitute administrative proceedings; take any additional action that it deems appropriate; and pursue any and all violations, maximum penalties, injunctive relief, or other relief that FinCEN deems appropriate. FinCEN may take any such action even if it did not take such action against Binance in this Consent Order and notwithstanding the releases and waivers herein. In the event FinCEN takes such action under this paragraph, Binance

specifically agrees to toll any applicable statute of limitations and to waive any defenses based on a statute of limitations or the passage of time that may be applicable to the Statement of Facts in this Consent Order, until a date 180 days following Binance's receipt of notice of FinCEN's determination that a misrepresentation or breach of this agreement has occurred, except as to claims already time barred as of the Effective Date of this Consent Order.

In the event that FinCEN determines that Binance has made a misrepresentation or failed to comply with this Consent Order, or any portion thereof, all statements made by or on behalf of Binance to FinCEN, including the Statement of Facts, whether prior or subsequent to this Consent Order, will be admissible in evidence in any and all proceedings brought by or on behalf of FinCEN. Binance agrees that it will not assert any claim under the Constitution of the United States of America, Rule 408 of the Federal Rules of Evidence, or any other law or federal rule that any such statements should be suppressed or are otherwise inadmissible. Such statements shall be treated as binding admissions, and Binance agrees that it shall be precluded from disputing or contesting any such statements. FinCEN shall have sole discretion over the decision to impute conduct or statements of any director, officer, employee, agent, or any person or entity acting on behalf of, or at the direction of Binance in determining whether Binance has violated any provision of this Consent Order.

XII. PUBLIC STATEMENTS

Binance agrees that it shall not, nor shall its attorneys, agents, partners, directors, officers, employees, affiliates, or any other person authorized to speak on its behalf or within its authority or control, take any action or make any public statement, directly or indirectly, contradicting its admissions and acceptance of responsibility or any terms of this Consent Order, including any fact finding, determination, or conclusion of law in this Consent Order.

FinCEN shall have sole discretion to determine whether any action or statement made by Binance, or by any person under the authority, control, or speaking on behalf of Binance contradicts this Consent Order, and whether Binance has repudiated such statement.

XIII. RECORD RETENTION

In addition to any other record retention required under applicable law, Binance agrees to retain all documents and records required to be prepared or recorded under this Consent Order or otherwise necessary to demonstrate full compliance with each provision of this Consent Order, including supporting data and documentation. Binance agrees to retain these records for a period of 6 years after creation of the record, unless required to retain them for a longer period of time under applicable law.

XIV. SEVERABILITY

Binance agrees that if a court of competent jurisdiction considers any of the provisions of this Consent Order unenforceable, such unenforceability does not render the entire Consent Order unenforceable. Rather, the entire Consent Order will be construed as if not containing the particular unenforceable provision(s), and the rights and obligations of FinCEN and Binance shall be construed and enforced accordingly.

XV. SUCCESSORS AND ASSIGNS

Binance agrees that the provisions of this Consent Order are binding on its owners, officers, employees, agents, representatives, affiliates, successors, assigns, and transferees to whom Binance agrees to provide a copy of the executed Consent Order. Should Binance seek to sell, merge, transfer, or assign its operations, or any portion thereof, that are the subject of this Consent Order, Binance must, as a condition of sale, merger, transfer, or assignment obtain the written agreement of the buyer, merging entity, transferee, or assignee to comply with this Consent Order.

XVI. MODIFICATIONS AND HEADINGS

This Consent Order can only be modified with the express written consent of FinCEN and Binance. The headings in this Consent Order are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Order or its individual terms.

XVII. AUTHORIZED REPRESENTATIVE

Binance's representative, by consenting to and approving this Consent Order, hereby represents and warrants that the representative has full power and authority to consent to and approve this Consent Order for and on behalf of Binance, and further represents and warrants that Binance agrees to be bound by the terms and conditions of this Consent Order.

XVIII. NOTIFICATION

Unless otherwise specified herein, whenever notifications, submissions, or communications are required by this Consent Order, they shall be made in writing and sent via first-class mail and simultaneous email, addressed as follows:

To FinCEN: Associate Director, Enforcement and Compliance Division
Financial Crimes Enforcement Network
P.O. Box 39, Vienna, Virginia 22183

To Binance: Binance Holdings Limited
c/o Gibson, Dunn & Crutcher LLP
1050 Connecticut Avenue, N.W.,
Washington, DC 20036

Notices submitted pursuant to this paragraph will be deemed effective upon receipt unless otherwise provided in this Consent Order or approved by FinCEN in writing.

XIX. COUNTERPARTS

This Consent Order may be signed in counterpart and electronically. Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

XX. EFFECTIVE DATE AND CALCULATION OF TIME

This Consent Order shall be effective upon the date signed by FinCEN. Calculation of deadlines and other time limitations set forth herein shall run from the effective date (excluding the effective date in the calculation) and be based on calendar days, unless otherwise noted, including intermediate Saturdays, Sundays, and legal holidays.

By Order of the Director of the Financial Crimes Enforcement Network.

/s/_____
Andrea Gacki Date:
Director

Consented to and Approved By:

/s/_____
Joshua Eaton
Deputy General Counsel
Binance Holdings Limited,
Binance (Services) Holdings Limited,
Binance Holdings (IE) Limited

ATTACHMENT A

INDEPENDENT COMPLIANCE MONITOR

The duties and authority of the Monitor, and the obligations of Binance, on behalf of itself, its subsidiaries, and its affiliates, with respect to the Monitor and FinCEN, are as described below:

1. Binance shall retain the Monitor for a period of five years (the Term of the Monitorship), unless the early termination or extension provisions of Paragraph 4 of Section VI.A of the Consent Order is triggered.

Monitor's Mandate

2. The Monitor's primary responsibility is, in the manner set forth below, to: (i) assess and monitor Binance's compliance with the terms of the Consent Order, including completion of the Undertakings set forth in Section VI, so as to specifically address and reduce the risk of any recurrence of Binance's misconduct; (ii) evaluate the effectiveness of Binance's compliance with Relevant BSA Provisions and related implementing regulations applicable to MSBs, except with respect to any reporting requirements on an ongoing basis for transactions effected as of and after the date of the Consent Order (*i.e.*, such exception to MSB reporting obligations does not apply to reports that Binance is required to file pursuant to the SAR Lookback described in Section VI.C); (iii) assess and monitor senior management's commitment to, and effective implementation of, Binance's AML and sanctions compliance programs; and (iv) assess and monitor Binance's compliance with the applicable terms of the settlement agreement between Binance and OFAC, the consent order between Binance and the CFTC, as well as the applicable terms of Binance's plea agreement with the Department of Justice (collectively, the Mandate).

Binance's Obligations

3. Binance shall cooperate fully with the Monitor, and the Monitor shall have the authority to take such steps as, in their view, may be reasonably necessary to be fully informed about Binance's AML and sanctions compliance programs in accordance with the terms of the Consent Order and the animating principles thereof, subject to applicable law, including applicable data protection and labor laws and regulations. To that end, Binance shall: facilitate the Monitor's access to Binance's documents and resources; not limit such access, except as provided in Paragraphs 4–5; and provide guidance on applicable local law (such as relevant data protection and labor laws). Binance shall provide the Monitor with access to all information, documents, records, facilities, and employees, as requested by the Monitor, that fall within the scope of the Mandate of the Monitor under the Consent Order and this Attachment A, including, but not limited to, information related to Binance's announced exit from Russia initiated through the September 2023 transaction to sell its Russian business to CommEx. Binance shall use its best efforts to provide the Monitor with access to Binance's former employees and its third-party vendors, agents, consultants, contractors, and subcontractors.

Withholding Access

4. The parties agree that no attorney-client relationship shall be formed between Binance and the Monitor. In the event that Binance seeks to withhold from the Monitor access to information, documents, records, facilities, or current or former employees of Binance that may be subject to a claim of attorney-client privilege or to the attorney work-product doctrine, or where Binance reasonably believes production would otherwise be inconsistent with applicable law, Binance shall work cooperatively with the Monitor to resolve the matter to the satisfaction of the Monitor.

5. If the matter cannot be resolved, at the request of the Monitor, Binance shall promptly provide written notice to the Monitor and FinCEN. Such notice shall include a general description of the nature of the information, documents, records, facilities or current or former employees that are being withheld, as well as the legal basis for withholding access. FinCEN reserves the right to seek to compel access to such information, documents, records, facilities, or employees.

Monitor's Coordination with Binance and Review Methodology

6. In carrying out the Mandate, to the extent appropriate under the circumstances, the Monitor should coordinate with Binance's personnel, including in-house counsel, compliance personnel, internal auditors, and the SAR Lookback and AML Program Consultants engaged to complete the SAR Lookback and AML Program Reviews set forth in Sections VI.C and VI.D, respectively, of the Consent Order on an ongoing basis. In carrying out the Mandate, the Monitor shall propose the selection of the SAR Lookback and AML Program Consultants, and maintain the right to veto the engagement of a proposed independent consultant that the Monitor deems unsuitable to complete the SAR Lookback and AML Program Reviews.[89] The Monitor may rely on the product of Binance's processes, including but not limited to studies, reviews, sampling and testing methodologies, audits, and analyses conducted by or on behalf of Binance, as well as Binance's internal resources (*e.g.*, legal, compliance, and internal audit), which can assist the Monitor in carrying out the Mandate, provided that the Monitor has confidence in the quality of those resources. In this regard, the Monitor may consider the SAR Lookback and AML Program Reviews, as well as any other independent consultants that Binance voluntarily engages to assist

[89] Subject to FinCEN approval, the Monitor may elect to conduct either one or both of the SAR Lookback Review and AML Program Review.

in its compliance with the Relevant BSA Provisions.

7. Subject to the specific requirements set forth in Sections VI.C and VI.D of the Consent Order to oversee the SAR Lookback and AML Program Reviews, the Monitor's reviews should use a risk-based approach, and thus, the Monitor is not expected to conduct a comprehensive review of all business lines, all business activities, or all markets. In carrying out the Mandate, the Monitor should consider, for instance, risks presented by: (i) the particular markets in which Binance offers its products and services; (ii) the types of CVC products and services, including AECs, that Binance offers its customers; (iii) the status and strength of Binance's controls to identify and report suspicious transactions; (iv) the customer identification and verification policies applied to users accessing Binance, including the application of such controls to subaccounts; (v) the number, type, and frequency of alerts that have been triggered by types or groups of customers and how Binance has handled those alerts; (vi) the sufficiency of the AML-related personnel and resources within the compliance function; (vii) the status and strength of Binance's geofencing controls, including to ensure that Binance fully exits from the United States, as well as the extent to which such geofencing controls effectively incorporate relevant information about users indicating their accessing Binance services through a VPN or similar service to obscure their location in a particular jurisdiction; and (viii) other required components of the Consent Order, the settlement agreement between Binance and OFAC, the consent order between Binance and the CFTC, and the applicable terms of Binance's plea agreement with the Department of Justice.

8. In undertaking the reviews described below to carry out the Mandate, the Monitor shall formulate conclusions based on, among other things: (a) inspection of relevant documents, including Binance's current policies and procedures; (b) on-site observation of selected systems

and procedures of Binance at sample sites, including transaction monitoring, record-keeping, and internal audit procedures; (c) meetings with, and interviews of, relevant current and, where appropriate, former directors, officers, employees, business partners, agents, and other persons at mutually convenient times and places; (d) analyses, studies, and testing of Binance's AML and sanctions compliance programs; and (e) the SAR Lookback and AML Program Reviews.

Monitor's Written Work Plans

9. To carry out the Mandate, during the Term of the Monitorship, the Monitor shall conduct an initial scoping review (First Review) and prepare a first report (First Report), followed by at least four follow-up reviews and reports as described in Paragraphs 12–17 below. With respect to the First Report, after consultation with Binance and FinCEN, the Monitor shall prepare the first written work plan within 60 days of being retained, and Binance and FinCEN shall provide comments within 30 days of receipt of the written work plan. The first written work plan must describe: (i) the proposed parameters, high-level timelines, and key dependencies associated with the SAR Lookback and AML Program Reviews, including the scope of such undertakings and the Monitor's proposed oversight of the SAR Lookback and AML Program Consultants; and (ii) a plan to assess and monitor Binance's compliance with the applicable terms of the settlement agreement between Binance and OFAC, and the consent order between Binance and the CFTC. With respect to each follow-up report, after consultation with Binance and FinCEN, the Monitor shall prepare a written work plan at least 30 days prior to commencing a review, and Binance and FinCEN shall provide comments within 20 days after receipt of the written work plan. Any disputes between Binance and the Monitor with respect to any written work plan shall be decided by FinCEN in its exclusive discretion.

10. All written work plans shall identify with reasonable specificity the activities the

Monitor plans to undertake in execution of the Mandate, including a written request for documents, as applicable. The Monitor's work plan for the first review shall include such steps as are reasonably necessary to conduct an effective first review in accordance with the Mandate, including by: (i) developing an understanding, to the extent the Monitor deems appropriate, of the facts and circumstances surrounding any violations of the BSA that occurred before the date of the Consent Order; and (ii) using that understanding to recommend changes to the scope of the SAR Lookback and AML Program Reviews. In developing an understanding of Binance's historical violations of the BSA, the Monitor is to rely, to the extent possible, on available information and documents provided by Binance. The Monitor need not conduct its own inquiry into the historical events that gave rise to the Consent Order except as otherwise necessary to fulfill the Mandate.

First Review

11. The First Review shall commence no later than 90 days from the date of the engagement of the Monitor (unless otherwise agreed by FinCEN). The Monitor shall issue a written report (First Report) within 90 days of commencing the first review, setting forth: (i) the scope of the AML Program and SAR Lookback Reviews, including applicable requirements set forth in Sections VI.C and VI.D of the Consent Order, (ii) any other work designed to enhance Binance's program for ensuring compliance with the Relevant BSA Provisions, and (iii) any applicable reporting requirements set forth in Binance's consent order with the CFTC and settlement agreement with OFAC. The Monitor should consult with Binance concerning the Monitor's findings and recommendations on an ongoing basis and should consider Binance's comments and input to the extent the Monitor deems appropriate. The Monitor may also choose to share a draft of their reports with Binance prior to finalizing them. The Monitor's reports need not recite or describe comprehensively Binance's history or compliance policies, procedures, and

practices, but rather may focus on those areas with respect to which the Monitor wishes to make recommendations, if any, for improvement or which the Monitor otherwise concludes merit particular attention. The Monitor shall provide its reports to Binance's senior management and contemporaneously transmit copies to:

Associate Director, Enforcement and Compliance Division
Financial Crimes Enforcement Network
P.O. Box 39, Vienna, Virginia 22183

Associate Director for Enforcement, Compliance, and Analysis
Office of Foreign Assets Control
Freedman's Bank Building, U.S. Department of the Treasury
1500 Pennsylvania Ave, N.W., Washington, D.C. 20220.

Deputy Director
Commodity Futures Trading Commission, Chicago Regional Office
Ralph Metcalfe Federal Building
77 West Jackson Blvd., Ste. 800
Chicago, IL 60604

After consultation with Binance, the Monitor may extend the time period for issuance of the first report for a brief period of time with prior written approval of FinCEN.

Follow-Up Reviews

12. A follow-up, implementation plan review (Second Review) shall commence no later than 90 days after AML Program Consultant has made its recommendations to Binance (unless otherwise agreed by FinCEN). The Monitor shall issue a written second report (Second Report) within 60 days of commencing the Second Review, setting forth the Monitor's assessment and, if necessary, making recommendations in the same fashion as set forth in Paragraph 11, with respect to: (i) Binance's plan to execute the Implementation Plan, and (ii) Binance's compliance with the applicable terms of the settlement agreement with OFAC, including the Compliance Commitments described therein, and any applicable reporting requirements set forth in Binance's

consent orders with the CFTC. After consultation with Binance, the Monitor may extend the time period for issuance of the Second Report for a brief period of time with prior written approval of FinCEN.

13. Within 60 days after receiving the Monitor's Second Report, Binance shall finalize its plan to implement within 180 days all recommendations in the report, unless, within 30 days after receiving the report, Binance notifies in writing the Monitor and FinCEN concerning any recommendations that Binance considers unduly burdensome, inconsistent with applicable law or regulation, impractical, excessively expensive, or otherwise inadvisable. With respect to any such recommendation, Binance need not incorporate that recommendation into the plan to implement all recommendations but shall propose in writing to the Monitor and FinCEN an alternative policy, procedure, or system designed to achieve the same objective or purpose. As to any recommendation on which Binance and the Monitor do not agree, such parties shall attempt in good faith to reach an agreement within 30 days after Binance serves the written notice.

14. In the event Binance and the Monitor are unable to agree on an acceptable alternative proposal, Binance shall promptly consult with FinCEN. FinCEN, after consultation with OFAC and the CFTC, as appropriate, may consider the Monitor's recommendation and Binance's reasons for not adopting the recommendation in determining whether Binance has fully complied with its obligations under the Consent Order. Pending such determination, Binance shall not be required to implement any contested recommendation(s).

15. The Monitor shall undertake a follow-up, validation review (Third Review) not later than 60 days after the date by which all SAR filings have been as required by the SAR Lookback Review. The Monitor shall issue a third report within 180 days of commencing the review, which shall focus on: (i) validating the work that Binance undertook to satisfy all recommendations

resulting from the AML Program and SAR Lookback Reviews, (ii) remediating any new issues that the Monitor identifies during the course of the Third Review, including, but not limited to, the required elements of the Consent Order, and (iii) Binance's compliance with the applicable terms of the settlement agreement with OFAC, including the Compliance Commitments described therein, and any applicable reporting requirements set forth in Binance's consent orders with the CFTC (Third Report). The recommendations of the Third Report shall follow the same procedures described in Paragraphs 13–14.

16. The Monitor shall undertake a follow-up, re-validation review (Fourth Review) not later than 240 days after the issuance of the Third Report. The Monitor shall issue a fourth report within 120 days of commencing the Fourth Review, which shall focus on: (i) validating the additional work that Binance undertook to satisfy the recommendations from the Third Review, (ii) remediating any new issues that the Monitor identifies during the course of the Fourth Review, including, but not limited to, the required elements of the Consent Order, and (iii) Binance's compliance with the applicable terms of the settlement agreement with OFAC, including the Compliance Commitments described therein, and any applicable reporting requirements set forth in Binance's consent orders with the CFTC (Fourth Report). The recommendations of the Fourth Report shall follow the same procedures described in Paragraphs 13–14.

17. Following the Fourth Review, the Monitor shall complete a final, certification review (Fifth Review) to: (i) determine whether the Monitor is able to certify that Binance's AML program, including its policies and procedures and internal controls, is reasonably designed and implemented to prevent and detect violations of the Relevant BSA Provisions, and (ii) Binance's compliance with the applicable terms of the settlement agreement with OFAC, including the Compliance Commitments described therein, and any applicable reporting requirements set forth

in Binance's consent orders with the CFTC. The Fifth Review and resulting report, including, if applicable, the accompanying certification, shall be completed and delivered to FinCEN no later than 30 days before the end of the Term.

Monitor's Discovery of Potential or Actual Misconduct

18. Except as set forth below in paragraphs (19), (20), and (21), should the Monitor discover during the course of their engagement that any director, officer, employee, agent, third-party vendor, or consultant of Binance may have engaged in unlawful activity in violation of the BSA or OFAC regulations (Potential Misconduct), the Monitor shall immediately report the Potential Misconduct to Binance's General Counsel and Chief Compliance Officer for further action, unless the Potential Misconduct was already so disclosed. The Monitor also may report Potential Misconduct to FinCEN (and OFAC, as appropriate) at any time, and shall report Potential Misconduct to FinCEN (and OFAC, as appropriate) upon request.

19. In some instances, the Monitor should immediately report Potential Misconduct directly to FinCEN (and OFAC, as appropriate) and not to Binance. The presence of any of the following factors militates in favor of reporting Potential Misconduct directly to FinCEN (and OFAC, as appropriate) and not to Binance, namely, where the Potential Misconduct: (i) poses a risk to public health or safety or the environment; (ii) involves senior management of Binance; (iii) involves obstruction of justice; or (iv) otherwise poses a substantial risk of harm.

20. If the Monitor believes that any Potential Misconduct has occurred or may constitute a criminal or civil violation (Actual Misconduct), the Monitor shall immediately report Actual Misconduct to FinCEN (and OFAC, as appropriate). When the Monitor discovers Actual Misconduct, the Monitor shall disclose the Actual Misconduct solely to FinCEN (and OFAC, as appropriate), and, in such cases, disclosure of the Actual Misconduct to the General Counsel or

Chief Compliance Officer of Binance should occur as FinCEN and the Monitor deem appropriate under the circumstances.

21. The Monitor shall address in their reports the appropriateness of Binance's response to disclosed Potential Misconduct or Actual Misconduct, whether previously disclosed to FinCEN (and OFAC, as appropriate) or not. Further, if Binance or any entity or person working directly or indirectly for or on behalf of Binance withholds information necessary for the performance of the Monitor's responsibilities and the Monitor believes that such withholding is without just cause, the Monitor shall also immediately disclose that fact to FinCEN and address Binance's failure to disclose the necessary information in their reports.

22. Neither Binance nor anyone acting on its behalf shall take any action to retaliate against the Monitor for any such disclosures or for any other reason.

Meetings During Term of Monitorship

23. The Monitor shall meet with FinCEN within 30 days after providing each report to FinCEN to discuss the report, to be followed by a meeting between FinCEN, the Monitor, and Binance. OFAC, the CFTC, and the Department of Justice may choose to attend such meetings but will not be required to do so.

24. At least annually, and more frequently if appropriate, representatives from Binance and FinCEN will meet together to discuss the monitorship and any suggestions, comments, or improvements Binance may wish to discuss with or propose to FinCEN, including with respect to the scope or costs of the monitorship. OFAC, the CFTC, and the Department of Justice may choose to attend such meetings but will not be required to do so.

Contemplated Confidentiality of Monitor's Reports

25. The reports will likely include proprietary, financial, confidential, and competitive business information. Moreover, public disclosure of the reports could discourage cooperation, or impede pending or potential government investigations and thus undermine the objectives of the monitorship. For these reasons, among others, the reports and the contents thereof are intended: (i) to be made available to only FinCEN, OFAC, the CFTC, and the Department of Justice; and (ii) to remain non-public, except as otherwise agreed to by the parties in writing, or except to the extent that FinCEN determines in its exclusive discretion that disclosure would be in furtherance of FinCEN's discharge of duties and responsibilities, or is otherwise required by law.